# Exhibit 2

Bloomberg
GOVERNMENT

# Senate Permanent Select Intelligence Committee hearing on the SolarWinds Hack, sked FINAL

February 24, 2021 12:45PM ET

TRANSCRIPT

February 23, 2021

COMMITTEE HEARING

SEN. MARK WARNER, D-VA.

SENATE PERMANENT SELECT INTELLIGENCE COMMITTEE HEARING ON THE SOLARWINDS HACK

Bloomberg Government

Support: 1-877-498-3587

www.bgov.com

SENATE PERMANENT SELECT INTELLIGENCE COMMITTEE HEARING ON THE SOLARWINDS HACK

FEBRUARY 23, 2021

SPEAKERS:

SEN. MARK WARNER, D-VA., CHAIRMAN

SEN. RON WYDEN, D-ORE.

SEN. MARTIN HEINRICH, D-N.M.

SEN. DIANNE FEINSTEIN, D-CALIF.

SEN. MICHAEL BENNET, D-COLO.

SEN. ANGUS KING, I-MAINE

SEN. BOB CASEY, D-PA.

SEN. KIRSTEN GILLIBRAND, D-N.Y.

SEN. CHARLES E. SCHUMER, D-N.Y., EX OFFICIO

SEN. JACK REED, D-R.I., EX OFFICIO

SEN. MARCO RUBIO, R-FLA., VICE CHAIRMAN

SEN. RICHARD M. BURR, R-N.C.

SEN. JIM RISCH, R-IDAHO

SEN. SUSAN COLLINS, R-MAINE

SEN. ROY BLUNT, R-MO.

SEN. TOM COTTON, R-ARK.

SEN. JOHN CORNYN, R-TEXAS

SEN. BEN SASSE, R-NEB.

SEN. MITCH MCCONNELL, R-KY., EX OFFICIO

SEN. JAMES M. INHOFE, R-OKLA., EX OFFICIO

WITNESSES:

SUDHAKAR RAMAKRISHNA, PRESIDENT AND CEO OF SOLARWINDS

KEVIN MANDIA, CEO OF FIREEYE

BRAD SMITH, PRESIDENT OF MICROSOFT

GEORGE KURTZ, PRESIDENT AND CEO OF CROWDSTRIKE

WARNER: Good afternoon, everyone. I'd like to call this hearing to order and apologize to our witnesses and others with COVID. And a vote has just been called. We're going to a little bit be playing this by ear.

So, I'm going to make my opening statement, ask the Vice-Chairman to make his opening statement. We'll be monitoring the vote which just opened a moment ago. We've got two, so we'll either tag team through this or take a five-minute recess to get us some -- all a chance to go vote on both these items.

First, I'd like to take this opportunity to welcome our two new members, one of which I think is at least on Zoom, Senator Casey, but also Senator Gillibrand to the committee.

I work for -- look forward to working with both of you as members of the Senate Intelligence Committee in the bipartisan tradition of this committee. The Intelligence Committee's record of working together in the interest of America's national security has been due in no small part to the tireless efforts of our Former Chairman, Senator Burr and our new Vice-Chairman, Senator Rubio.

So, I want to take this opportunity during my first hearing as Chairman to thank you for your partnership and friendship. I'm confident that we'll be able to keep working together in a bipartisan way in the 117th Congress.

I'd also very much like to welcome our witnesses today: Kevin Mandia, CEO of FireEye; Sudhakar Ramakrishna, President and CEO of SolarWinds; Brad Smith, President of Microsoft; and I believe remotely George Kurtz, President and CEO of CrowdStrike.

I would like, for the record, to note that we also asked a representative from Amazon Web Services to join us today, but unfortunately they declined. But we will be expecting to get a full update. We've had one update from our friends at Amazon, but it would be most helpful if in the future they actually attended these hearings.

Today's hearing is on the widespread compromise of public and private computer networks in the United States by a foreign adversary, colloquially or commonly called the 'SolarWinds hack'.

While most infections appear to have been caused by a trojanized update of SolarWinds Orion software, further investigations have revealed additional victims who do not use SolarWinds tools. It has become clear that there's much more to learn about this incidence, its causes, its scope and scale and where we go from here.

This is the second hearing this committee has held on this topic. Our first was the closed hearing on the now infamous January 6th with government officials responding to the incident. It's going to take the combined power of both the public and private sector to understand and respond to what happened. Preliminary indications suggest that the scope and scale of this incident are beyond any that we've confronted as a nation and its implications are significant.

Even though what we've seen so far indicates this was carried out as an espionage campaign targeting more than a hundred or so companies and government agencies, the reality is, those hackers responsible have gained access to thousands of companies and the ability to carry out far more destructive operations if they'd wanted to.

And I want to repeat that. This intrusion had the possibility of being exponentially worse than what has come to pass so far. The footholds these hackers gained into private networks, including some of the world's largest IT vendors, may provide opportunities for future intrusions for years to come.

One of the reasons the SolarWinds hack has been especially concerning is that it was not detected by the multibillion dollar U.S. government cybersecurity enterprise or anyone else until the private security firm FireEye, and I want to again compliment our friend, Kevin Mandia who's appeared before this committee a number of times, on their own without a requirement to report actually publicly announced that it had detected a breach of its own network by a nation-state intruder.

A very big question looming in my mind is, had FireEye not detected this compromise in December and chosen on their own to come forward, would we still be in the dark today?

As Deputy National Security Advisor Anne Neuberger who's been chosen by the President to lead the response in this -- to this SolarWinds hack said last week, the response to this incident from both the public and private sector is going to take a long time. All of our witnesses today are involved in some aspect of the private sector response to this incident.

I want to hear from them on the progress so far, the challenges we'll need to overcome in order to fully expel these hackers and how we can prevent supply chain attacks like this in the future. I'd also like to hear from them about their experiences working with the federal government, namely the Unified Coordination Group in mitigating this compromise.

The SolarWinds hack was a sophisticated and multifaceted operation. A software supply chain operation that took advantage of trusted relationships with software providers in order to break into literally thousands of entities. Combined with the use of these sophisticated authentication exploits, it also leveraged vulnerabilities and major authentication protocols. Basically, granting the intruder the keys to the kingdom, allowing them to deftly move across both on premises and cloud-based services all while avoiding detection. While many aspects of this compromise are unique, the SolarWinds hack has also highlighted a number of lingering issues that we've ignored for too long. This presents us an opportunity for reflection and action.

A lot of people are offering solutions including mandatory reporting requirements, wider use of multifactor authentication, requiring a software bill of goods and significantly improving threat information sharing between the government and private sector.

I've got a number of questions, but there are three that I'd like to pose in my opening. One, why shouldn't we have mandatory reporting systems, even if those reporting systems require some liability protection so we can better understand and better mitigate future attacks.

As I've pointed out, Senator Collins was way ahead of all of us on this issue literally years and years ago when she and Senator Lieberman first put forward legislation that required this critical -- mandatory reporting on critical infrastructure.

There's an open question though on who should receive such report even if you put that mandatory reporting in place. Do we need something like the National Transportation Safety Board or other public/private entity that can immediately examine major breaches to see if we have a systemic problem and see, as we seem to, in this case?

I think there's also some truth to the idea that if a Tier I adversary, a foreign nation state sends their A-team against almost any ordinary company in the world, chances are they're going to get in. But that cannot be an excuse for doing nothing to build defenses and making it harder for them to be successful once inside an enterprise.

I'm very interested in hearing from the witnesses what they think our policy response should be and what solutions they will actually -- they think will actually improve cybersecurity and incident report in the United States. Beyond the immediate aspects of the SolarWinds hack are larger issues that this committee needs to consider.

Do we need to finally come to some agreement on common norms in cyberspace? Hopefully, again on an international basis that potentially are enforceable and at least says to our adversaries, "If you violate these norms, there will be known consequences."

For example, we have these norms in other conflicts. We have military conflict that exists but there's been, for some time, a norm that you don't knowingly bomb a hospital or bomb an ambulance that's got a Red Cross shield on it. Should we therefore consider efforts that subvert patching, which are all about fixing vulnerabilities, to be similarly off-limits?

Once again, I want to thank our witnesses for joining us today, both in person and remotely. I personally talked to nearly -- with nearly all of our witnesses, in some cases multiple times since this incident was first reported. I appreciate their transparency and willingness to be part of this conversation.

After our witnesses conclude their remarks, we'll move to a round of five-minute questions based upon order of arrival. As a reminder to my colleagues, this incident is not over, so too are the criminal investigations by the FBI, so there might be some questions our witnesses cannot answer.

However, I'm confident they will be -- we'll get those answers at some point as we move forward. I now recognize the Vice-Chairman for his statement.

RUBIO: Thank you, Mr. Chairman and thanks for convening this hearing. And I'd like to welcome our witnesses from Microsoft and FireEye, SolarWinds, CrowdStrike, who are here to help the committee's examination of what is the largest cyber supply chain operation ever detected. So, we really do appreciate you being with us.

As the Chairman mentioned, we would -- we had extended an invitation to Amazon to participate. This operation we'll be discussing today used their infrastructure at least in part required it to be successful. Apparently, they were too busy to discuss that here with us today, and I hope they'll reconsider that in the future.

This operation involved, as already been said, the modification of the SolarWinds Orion platform which is a widely used software product. It included a malicious backdoor that was downloaded, my understanding up to 18,000 customers between March and June of last year.

But the most insidious part of this operation was that it hijacked the very security advice promulgated by security -- by computer security professionals to verify and apply patches as they are issued. So, there are many concerning aspects to this, first of its kind, at least at this scale operation that raised significant questions.

My understanding is that if FireEye had not investigated an anomalous event within their own network in November of last year, it's possible this would be a continuing and unfettered operation to this day.

I think everyone's asking, despite the investment that's been made in cybersecurity collectively between the government and the private sector, how no one detected this activity earlier. As it appears that they have been in the system for close to six -- five to six months before it was detected. Maybe even longer, closer to a year.

But the bottom line question is, how did we miss this and what are we still missing and what do we need to do to make sure that something like this using these sorts of tools never happen again.

Second, I think there's great interest in knowing exactly what these actors did. Based on what we know, to include what the government has stated publicly, the actor seems to have undertaken follow-on operations against a very small subset of the 18,000 networks to which they potentially had access.

So, aside from the mechanical aspects of removing a hacker from a network, what do we know about why these actors chose the targets that they did? What actions did they undertake within those networks? And what do we know that we do not know?

I always love that question. What do we know what we do not know? In essence, what are the open questions now and in the future about these sorts of tools on how they could be used or what do we still have open-ended that we are not able to answer at this time? And perhaps most importantly, who has the single comprehensive view of the totality of activity undertaken?

And that's another thing that everyone has struggled with, is who can see the whole field here on this? And third, what is it going to take to rebuild and have confidence in our networks?

And speaking with several of you in the days leading up to this, one of the hallmarks of this operation was the great care that was taken by this adversary to use bespoken infrastructure and tradecraft for each victim. Unlike other malware or ransomware cleanup operations, there is no template here that can be used for remediation. So, what's it going to take to have confidence in both government and in the private sector networks again?

Fourth, what do we need to do to raise the bar for the cybersecurity of this nation? Is cyber deterrence and achievable goal, how do we need to enhance cyber security information logging and sharing across the spectrum to protect against APTs in the future?

And finally though, this is a question for the government rather than the witnesses here today. I think it's important for this committee to ask itself and to inform the Members of the Senate what does the United States government need to do to respond to this operation?

Government officials initially stated this was an intelligence gathering operation. Just recently, however, the White House stated, "When there is a compromise of this scope and scale both across government and across the U.S. technology sector to lead to follow-on intrusions, it is more than a single incident of espionage. It is fundamentally of concern for the ability for this to become disruptive."

While I share this concern that an operation of this scale with the disruptive attempt could have caused mass chaos, those are not the facts that are in front of us. Everything we have seen thus far indicate that, at some level, this was an intelligence operation and a rather successful one that was ultimately disrupted.

While there are a myriad of ways for sovereign states to respond, I caution against the use of certain terms at this time until the facts lead us to the use of terms such as attack and so forth. I always advocate for standing up to our adversaries. I think that's important. I will continue to advocate for that, but I want to know today what the actor's intent seems to be and to the extent of damage before we categorize it, it may very well reach that level.

This committee and the rest of the Congress should consider what policies we need to pursue to better defend our nation's critical networks. In order to get a fuller view of the problem, perhaps we should consider mandating certain types of reporting, as the Chairman already mentioned, as it relates to cyber-attacks.

We must improve the information sharing that -- of this, there is no doubt between the federal government and private sector and I look forward to being an active and constructive participant in these debates on these new issues, as I know every member on this committee is.

And with that, I again want to welcome you and thank you for the testimony and the insights that you will share with us and the American people. It is important that the public understand the current, the persistent information conflict that the United States finds itself in against nation-state adversaries like Russia, but also like China and Iran and North Korea.

So, thank you, Mr. Chairman.

WARNER: Thank you, Senator Rubio. I think we're going to go ahead and we'll just trade off. I believe the order of the speakers is going to be FireEye, SolarWinds, Microsoft and CrowdStrike.

So Kevin, if you want to start us off, that'd be great. Turn on your -- I think you got to get your mic on.

MANDIA: Thank you, Mr. Chairman, Ranking Member Rubio, and the rest of the Members of the Senate Intelligence Committee. It is a privilege to be here with the opportunity to speak with you. And as the first witness, I'm going to discuss what happened from a firsthand experience as a Stage 2 victim to this intrusion.

I have opinions on who did it, I have opinions on what to do about it. But in the next four minutes, I don't have enough time to get through all that, so I look forward to your questions.

On background, I just want to give you a little background on FireEye. Responding to breaches is what we do for a living. We have a whole bunch of Quin-C type people that do forensics 2000 hours a year, and people hire us to figure out what happened and what to do about when they have a security breach.

We responded to over 1000 breaches in 2020. It was a tough year for Chief Information Security Officers. And as I sit here right now testifying to you, we're responding to over 150 computer security breaches. In short, this is what we do for a living. And what we're going to tell you today, we tell you with high confidence and high fidelity on the intent of the attackers and what they did.

So now, I want to present kind of the anatomy of this attack. We're referring to it as the 'SolarWinds campaign' but it's a little bit broader than that. Whoever this threat actor is, and we all pretty much know who it is, this has been a multi-decade campaign for them. They just so happened to, in 2020, create a backdoor SolarWinds implant.

So, the first part of this ongoing saga, Stage 1 of this campaign was you had to compromise SolarWinds. And the attackers did something there that was unique in that they didn't modify the source code there, they modified the build process, which to me, means this is a more portable attack than just at SolarWinds.

When you modify the build process, you're doing the last step of what happens before code becomes production for your buyers and customers, which just shows this is a very sophisticated attacker. And once they did that Stage 1 compromise with SolarWinds, we didn't find the implant till December of 2020. And it had been out there, if you look at the timeframe perspective, from March of 2020 and there was an update in June of 2020 as well.

But the attacker did something interestingly with the timing. They did a dry run in October of 2019 where they put a nocuous code into the SolarWinds build just to make sure the results of their intrusion was making it into the SolarWinds platform production environment.

Now, I'll explain how we found this implant, because there's no magic wand to say, "Where's the next implant?" When we were compromised, we were set up to do that investigation. It's what we do. We put almost 100 people on this investigation. Almost all of them had 10,000 hours, there's so to speak 10,000 hours of doing investigations and we unearthed every clue we could possibly find and we still didn't know, so how did the attacker break in?

So, we had to do extra work. And at some point in time after exhausting every investigative lead, the only thing left was the earliest evidence of compromise was a SolarWinds server and we had to tear it apart. And what I mean by that is we had to decompile it.

Specifically, there was 18,000 files in the update, 3500 executable files. We had over a million lines of assembly code. For those of you that haven't looked at assembly, you don't want to. It's something that you have to have specialized expertise to review, understand, piece apart. And we found the proverbial needle in the haystack, an implant.

But how did we get there? Thousands of hours of humans investigating everything else. And that's one of the reasons I share that is, you wonder why people missed it, this was not the first place you'd look. This was the last place you'd look for an intrusion.

Over 17,000 companies were compromised by that implant. So, Stage 1 was the compromise SolarWinds, get an implant in and indiscriminately went to the 17,000 folks that downloaded it. That means the attackers had a menu of 17,000 different companies.

Stage 2 of this attack was the companies that these attackers intended to do additional action on. And I want to talk about what they did during Stage 2 victims. And I want to kind of say, Stage 1, the attacker hasn't done anything more than crack open the window into a company, but they haven't gone into the house to rob anything yet.

Stage 2, they go into the house to rob it. When we look at the Stage 2 threat actor -- or Stage 2 victims, this is where Microsoft's top-down viewpoint from their cloud, where there was a lot of activity, comes up with approximately 60 victim organizations and we read that the government's aware of about 100 organizations.

For us, being a Stage 2, we had firsthand account of what they do. The attackers came in through the SolarWinds implant and the very first thing they did is went for your keys, your tokens. Basically, they stole your identity architecture so they could access your networks the same way your people did.

If it's -- and that's why this attack was hard to find because these attackers, from Day 1, they had a backdoor, imagine almost a secret door into your house and the first thing that happens when they come to that secret door is all of your keys are right there. They just grab them, and now, they can get in to any locks you have in your house the same way your people do.

And I think during a pandemic where everybody's working from home, it's way harder to detect an attack like this where the only indicator of compromise was just somebody logging in as one of your employees and there's nothing else far-fetched about that.

Right after they got our valid credentials, our two-factor authentication mechanisms bypassed, they went to our O365 environment. And whether it was O365 or something else, I've had enough experience over my 25 years of responding to breaches to know this group targets specific people almost like they have collection requirements.

So, there they targeted e-mails and documents. So, Stage 2, it was get credentials so you could log in, get the keys to the safety deposit boxes. Stage -- the next step, Step 2 of that was access e-mail, access documents with said keys. And then, the third thing was dependent on who you were and what you did and what industry you were as a victim but it's primarily what I put in the other category, steal source code, steal software, in the case of FireEye, take some of our Red Teaming tools that we use to assess people's security programs.

Bottom line, exceptionally hard to detect. And when I got my first briefing on this and reviewed the facts on Day 1, everything about this aligned to a threat actor who, it is my opinion, was more concerned about operational security than mission accomplished. And at the minute you could detect these folks and stop them breaking through the door, they sort of evaporated like ghosts until their next operation.

So with that, on behalf of FireEye, I'd like to thank all of you for the opportunity to set the stage for the other witnesses. I'm very excited to work with all of you and to my fellow witnesses and others in the private sector as well as the public sector, to advance our nation in defending ourselves in cyber space.

Now, I look forward to taking your questions. Thank you.

WARNER: Thank you, Kevin. Sudhakar?

RAMAKRISHNA: Chairman Warner, Vice-Chairman Rubio...

WARNER: I think you need to get your mic on or bring your mic a little closer.

RAMAKRISHNA: Chairman Warner, Vice-Chairman Rubio, and Members of the committee. On behalf of SolarWinds' employees, partners and customers in the U.S. and around the world, I would first like to say thank you for inviting us to this hearing.

By way of background, I'm Sudhakar Ramakrishna, and I joined SolarWinds on January 4th of this year. Prior to SolarWinds, I was with a company called Pulse Secure for over five years and previously held executive roles at other technology companies.

In my roles, I have been involved with cyber incidents and have seen firsthand the challenges they present as well as the opportunities they create for learnings and improvements. While our products and customers were the subject of this unfortunate and reckless operation, we take our obligation very seriously to work tirelessly to understand it better, to help our customers, and to be transparent with our learnings with our industry colleagues and the government.

SolarWinds started in 1999 in Oklahoma as a provider of network tools. And to this date, we have remained true to our mission of helping IT professionals solve their problems and manage their networks now through more than 90 products. Today, we remain a U.S. headquartered company with over 3,000 employees working extremely hard to deliver customer success.

When we learned of these attacks, our very first priority and that remains true today, was the safety and protection of our customers. Our teams worked incredibly hard and tirelessly to provide remediations within about 72 hours of knowing about these attacks. We also acted very quickly to disclose these events to the authorities while providing remediations and starting our investigations of what did we learn about this, who may have done it, and what exactly happened in the process of insertion into our Orion platform.

We believe the Orion platform was specifically targeted in this nation-state operation to create a backdoor into the IT environments of select customers as my colleague Kevin noted as well. The threat actor did this by adding malicious code which we call 'Sunburst' diversions released between March and June of 2020. In other words, a three-month window was when the code with the malicious Sunburst code was deployed.

I will note that this code has been removed and is no longer an ongoing threat to the Orion platform. Additionally, after extensive investigations, we have not found Sunburst in our more than 70 non-Orion products.

Perhaps the most significant finding to date in our investigation is what the threat actor used to inject Sunburst into other Orion platforms. This injector tool which we call 'Sunspot' was stealthily inserted into the automated build processes of Orion and was designed to work behind the scenes.

Sunspot, which we discovered, poses a grave risk of automated supply chain attacks through many software development companies since the software processes that SolarWinds uses is common across the industry. As part of our commitment to transparency, collaboration and timely communications, we immediately informed our government partners and published our findings with the intention that other software companies in the industry could potentially use the tool to detect possible current and future supply chain attacks within their software build processes.

We understand the gravity of the situation and are applying our learnings of Sunspot and Sunburst and sharing this work more broadly. Internally, we call these initiators 'Secure by Design'. And it's premised on Zero Trust principles and developing a best-in-class secure software development model to ensure our customers can have the utmost confidence in our solutions.

We have published these details regarding our sets in various blog posts. But in summary, they are focused on three primary areas. The first is further securing our internal infrastructure. The second is ensuring and expanding the security of our build environments. And third, ensuring the security and integrity of the products we deliver.

Given our unique experience, we are committed to not only leading the way with the respect to secure software development, but to share our learnings with the industry. While numerous experts have commented on the difficulties that these nation-state operations present to any company, we are embracing our responsibility to being an active participant in helping prevent these types of attacks.

Everyone at SolarWinds is committed to doing so, and we value the trust and confidence our customers place in us. Thank you again for your leadership in this very important matter. We appreciate the opportunity to share our experiences and our learnings. And I look forward to your questions. Thank you.

RUBIO: Thank you. And for the members who haven't yet voted, I guess everybody's voted because everybody's almost gone here. So, Mr. Smith, thank you for being here. We appreciate it.

SMITH: Well, thank you, Vice-Chairman Rubio and a huge thank you to you and Chairman Warner for bringing us altogether to discuss what's obviously such an important issue to the country, and I think, indeed to the world.

And I also just want to say thank you to Kevin and Sudhakar. It took the leadership, and I'll say, even the courage of companies like FireEye and SolarWinds to step forward and share information. And it is only through this kind of sharing of information that we will get stronger to address this.

I think Kevin and Sudhakar have done an excellent job of describing what happened, so I don't want to retrace the steps that they so ably took. Let me talk about two other things.

First, what does this mean? And second, what should we do?

Well, roughly 90 days or so since we first heard about this from Kevin's firm, from FireEye, I think we can step back and start to think about what it means.

First, we're dealing with a very sophisticated adversary. And Vice Chairman Rubio, I think your words of wisdom, of caution about avoiding certain labels are well put. But I do think we can say this, at this stage, we've seen substantial evidence that points to the Russian foreign intelligence agency and we have found no evidence that leads us anywhere else.

So, we'll wait for the rest of the formal steps to be taken by the government and others. But there's not a lot of suspense at this moment in terms of what we are talking about. It's very, very clear that this agency is very, very sophisticated. And as Kevin noted, that has been true for a long time. That is not new. But I think two other things are new. The first is the scale of this attack or hack or penetration or whatever we should call it.

At Microsoft, as we worked with customers that had been impacted by this, we stepped back and just analyzed all of the engineering steps that we had seen. And we asked ourselves, how many engineers did we believe had worked on this collective effort? And the answer we came to was, at least a thousand.

I should say, at least a thousand very skilled, capable engineers. So, we haven't seen this kind of sophistication matched with this kind of scale. But there is one other factor that I do believe puts this in a different category from what we have seen.

And, I think, even with the thoughtful consideration, it is appropriate to conclude even now this was an act of recklessness in my opinion. Why? Well, in part, I think, Chairman Warner put it very well.

The world relies on the patching and updating of software. We rely on it for everything. We relied on it, not only for the safety and health of our computers. We rely on it for our physical infrastructure, for hospitals and roads and airports because they all run on software.

To disrupt, to damage, to tamper with that kind of software updating process is in my opinion to tamper with what is in effect the digital equivalent of our public health service. It puts the entire world at greater risk.

And it was done, I think one must acknowledge in a very indiscriminate way. To seek to plant malware and distributed to 18,000 organizations around the world is in truth an act without clear analogy or precedent.

We've seen this done in Ukraine, but we haven't seen it done quite like this. It's a little bit like a burglar who wants to break into a single apartment but manages to turn off the alarm system for every home and every building in the entire city. Everybody's safety is put at risk and that is what we're grappling with here.

So what do we do? I think, we have to start by acknowledging and recognizing we need to do a lot. We all need to do a lot. We need to do a lot ourselves and we need to do a lot together.

Certainly, as Sudhakar was mentioning, we need to focus on the integrity, the protection of software build systems. The international data corporation estimates that there will be half a billion, 500 million software apps created in the next three or four years. That's half a billion build systems.

And it's not just software companies. It's banks. It's hospitals. It's governments. It's everyone that creates software. There are new steps that we will need to take to better secure and protect against the kind of attack that we saw here.

Second, I think we have a lot of work still to do, certainly across the United States when it comes to the modernization of our IT infrastructure. And to the application of IT best practices.

At Microsoft, we can only see this attack among our customers when it got to their use of their cloud services and all of the attacks that took place, took place on premise. Meaning a server that was in a serving room or a closet somewhere and it points to the fact that until we modernize and move more people to the cloud, we're going to be operating with less visibility than we should.

Third, we do need to enhance the sharing of threat intelligence. Now, that's the term in the cybersecurity community for information about attacks that people are seeing. And our basic challenge today is that that information too often exists in silos.

It exists in silos in the government. Exists in different companies. It doesn't come together. Fourth, I think because of that need, it is time. Not only to talk about, but to find a way to take action to impose in an appropriate manner some kind of notification obligation on entities in the private sector.

And so, of course, it's not a typical step when somebody comes and says, place a new law on me. Put it on ourselves. Put it on our customers. But I think it's the only way we're going to protect the country. And I think it's the only way we're going to protect the world.

And finally, I do believe it is time, it's maybe even overdue time, for us to look at the rules of the road. The norms and laws that if not every government is prepared to follow, at least the United States and our like-minded allies are prepared to step up and defend.

And among other things to say that this kind of tampering, indiscriminately and disproportionately with a software supply chain needs to be off limits. And there needs to be attribution. And there needs to be accountability as officials in the White House are now considering.

Finally, I'll close by addressing one question that Vice Chairman Rubio, I think, you posed, who knows the entirety of what happened here? One entity knows. It was the attacker. The attacker knows everything they did. And right now the attacker is the only one that knows everything that they did. We have pieces. We have pieces at Microsoft, SolarWinds, FireEye, CrowdStrike, others, we all have slices, people in the U.S. government.

But we need to bring those slices together and until we do, we'll be living and working and defending on an uneven playing field. That is not a recipe for success. But, let's also acknowledge one other thing. We know more than we did 100 days ago.

We are better informed. We are smarter and we can turn that knowledge into a resolve and action. That's what we need to do. That's what I hope the Congress can do. That's what, I think, the country and our allies need to do, if we use what we have learned, we can better protect our future. Thank you.

RUBIO: Thank you.

And finally, Mr. Kurtz, I believe he's on virtual?

KURTZ: Yes.

RUBIO: All right, excellent.

KURTZ: Thank you.

All right. Good afternoon, Chairman Warner, Ranking Member Rubio and members of the committee. Thank you for the opportunity to testify today. During my three-decade career in cybersecurity, I have seen firsthand the evolution of adversary techniques and have been at the forefront of developing the solutions to thwart them.

By the time I co-authored the original addition of Hacking Exposed in 1999, which later became the number one selling book in security, it was clear that organizations consistently failed to adequately defend themselves.

When I co-founded CrowdStrike in 2011, it was based on a conviction that the then-dominant approaches to security were no match for adaptive and well-resourced adversaries. We set out to elevate the industry's focus from stopping malware to preventing breaches regardless of their source.

My testimony today is based on my prior and current experiences, protecting thousands of organizations across the globe. I will begin by discussing our high level findings in the supply chain compromise and what lessons we might take away from it.

In mid-December, SolarWinds engaged our professional services team to perform incident response. Although, we had not worked with SolarWinds prior to this engagement nor had they used our software in the past, our teams collaborated effectively to investigate the breach, enhance their security posture and share actionable intelligence with the entire security community.

With their encouragement, we continue to coordinate and share findings with customers, industry partners, and federal agencies as appropriate.

Today, I would like to highlight a few significant capabilities this particular threat actor exhibited. Notably, the threat actor took advantage of systemic weaknesses in the Windows authentication architecture, allowing it to move laterally within the network as well as between the network and the cloud by creating false credentials, impersonating legitimate users and bypassing multifactor authentication.

The threat actor modified code within the development pipeline immediately prior to the software build, the final stage before source code become software. The threat actor leveraged unique IP addresses for command and control infrastructure for each of its victims, complicating investigations into the scope of the campaign but used common encryption methods and scrubbing techniques to avoid leaving behind unique indicators.

The threat actor was selective in activating the backdoors it implanted, purposefully selecting its victims from the wider universe of those who were vulnerable. With respect to attribution, CrowdStrike refers to this activity cluster behind these events, using the name StellarParticle.

We are aware that the U.S. government has stated this threat actor is likely of Russian origin. While we currently are unable to corroborate that finding, we have no information to suggest it is incorrect.

Regardless of attribution, there are a number of takeaways from these events. This campaign, in particular, emphasized the need to improve two important security disciplines, those involving supply chains and those involving security development.

StellarParticle is just the latest demonstration of supply chain attacks as a threat vector. This follows a number of previous high impact campaigns where the origins of attack are at the vendor level. With respect to software development, in addition to ensuring secure coding practices and adequate code review, organizations must protect their development platforms and code repositories at least as well as their enterprise environment.

Next, I would like to extend our considerations beyond this particular campaign and address six essential cybersecurity concepts and emerging technologies. The first is threat hunting. We know that the adversaries periodically breach even very well-defended enterprises. Properly trained and resourced defenders 00can find these bad guys and thwart their goals.

The second concept is speed. Every second counts to stop threat actors from achieving their objectives. Third is the power of machine learning prevention. The core of state-of-the-art cybersecurity solution is the ability to defeat novel threats, machine learning and artificial intelligence are essential.

Fourth is the need to enhance identity protection and authentication. As organizations further embrace cloud services and work from anywhere models, enterprise boundaries have continued to erode.

This trend increases the risk of relying upon traditional authentication methods and further weakens legacy security technologies. One of the most sophisticated aspects of the StellarParticle campaign was how skillful the threat actor took advantage of architectural limitations in Microsoft's Active Directory Federation Service.

The Golden SAML attack allowed them to jump from customer on premise environments and into cloud and cloud applications, effectively bypassing multifactor authentication. The specific attack vector was documented in 2017 and operates a cloud scale version of similar identity-based attacks I originally wrote about in 1999.

Moving to the fifth concept, let's touch upon principals of zero trust. Instead of authenticating to a network or device once and having ready access to everything that's connected, users must re-authenticate or otherwise establish permission for each new device or resource they wish to access. This reduces or prevents lateral movement and privilege escalation.

Finally, I will touch upon something known as XDR, which stands for Extended Detection and Response. Security teams demand contextual awareness and visibility from across their entire environment, including within cloud and ephemeral workloads.

As this Committee will appreciate XDR generates intelligence from what otherwise maybe no more than information overload. Each of these concepts apply equally to all organizations and regardless of size is a must.

The last point is critical. Often adversaries specifically target smaller organizations as a means to a greater end. This is part of the supply chain problem. We are proud that a number of security companies, including CrowdStrike are committed to offering comprehensive, easy to use solutions and manage security services to organizations of all size with varied budgets.

We also appreciate the need for improvements to government cybersecurity. Some of the most talented people in the field have worked or currently work in government organizations. Unfortunately, in many instances, our government colleagues are hobbled by legacy technologies, programs, complex procurement processes or complex obligations that detract from their core security work.

I realize that I've described a set of enormous challenges today, but I would like to close on a positive note. With CrowdStrike's visibility and to trillions of security events across thousands of customers globally, I'm encouraged by the silent victories the security community experiences every second of every day. Defenders face an endless evolving threat, but I remain optimistic that working together, we can prevail.

I hope my testimony today has offered some guidance on how we can accomplish that shared goal. CrowdStrike has its sleeves rolled up and is ready to continue to work with this committee and the greater security community to achieve success.

I would like to thank the committee for inviting me to testify today and for its leadership and I look forward to answering your questions, thank you.

RUBIO: Thank you, let me just begin, Mr. Kurtz by saying you've shown tremendous operational security behavior, though that backdrop you have in that video, you could be anywhere in the world. There's no way we can tell where you are just looking at that backdrop.

KURTZ: Absolutely.

RUBIO: All right. I'm going to get that backdrop. That is an awesome one. So let me ask you and Mr. Mandia the same question. So let me just say, everyone is familiar, I think the general public is familiar with cyber-attacks and hacks and the general guidance everyone is given is don't put some simple password like 1, 2, 3, 4.

They're easy to guess because we have seen they can guess it. There are all kinds of things out there also be able to crack them. Then, there's the infamous or the well-known phishing e-mail.

You get an e-mail. You click on it. They're in your system. These are all hardware type, sort of brute force intrusions. For folks at home, who may watch this later, trying to understand what the big deal about all this. This involves -- the other thing we're told that we need to do all the time, which is constantly upgrade the software.

Every time you get a software update, put it in, because it's got new security features. So, these guys get into that software update and you're basically, and it's almost like bringing them into your system under the guise of protecting you.

And that's what we are dealing with here today. And this has been a known vulnerability that something people knew was a theoretical possibility. It's my understanding this is the first time we've ever seen it at this scale and scope. And you'll correct me of your answer -- in your answer if I'm wrong.

The question I would have all of you, but really for Mr. Mandia and Kurtz is this is a sophisticated technique. This is not something that someone could do out of the basement of their home or is this something that could have eventually -- we could see it become widespread? What level of sophistication do you need to embed yourself in a software upgrade that ultimately winds up in someone's system?

MANDIA: George, if you don't mind, I'll jump on that first. And this was a planned attack. This is not something done in somebody's basement. There is somebody that thought about this. My gut is this attack started somewhere where somebody said if we wanted to compromise these entities, where is the supply chain?

They probably had a list of 5 to 10 companies. SolarWinds was one of them. And they figured out who can we get into? How do we do the implant? When they got into SolarWinds, they didn't just rush right to the implant. They wanted to make sure they could inject code first in the build process. That was in October of '19. Then four to five months later, they have an implant. In that four to five months, they designed an implant that masqueraded to look like SolarWinds traffic.

It was hard to pick up in the network. It had things in it in the malware -- malware, a lot of time you hear the word and you shut down. What are you going to say next? Well, this is what this malware did.

It slept for the first 11 days after it was installed. So, that if somebody did detect its beacon going out, they wouldn't be able to associate a beacon from the SolarWinds machine to the update they did randomly 11 days sooner.

Another thing it did is it looked for nearly 50 different products and shut them down when it ran. So, people are like, why didn't anybody detect the implant? It's because when it executed, it looked to see if CrowdStrike's agent was on the endpoint and FireEye's agent was on the endpoint, if Windows Defender was on the endpoint and it shut it off.

And it was -- and you don't make a backdoor as a bad guy, as a regular user. You make one as the root user or a system level backdoor. Senator Rubio, there's no doubt in my mind, this was planned. It was an operation. There are a lot of people involved. And the question really is, where's the next one? And when are we going to find it?

RUBIO: Mr. Kurtz, I'm guessing you probably agree with that assessment. So this is and all with little doubt a nation state actor. It would take that level of sophistication, is that right? Do both of you agree with that?

MANDIA (?): I do.

KURTZ (?): Yes.

RUBIO: Who? Who is that nation state actor? Or have you seen indications in it that tell you, this is who we believe it is?

MANDIA: George, you want to go first on that one?

KURTZ: Well, when we look at the adversaries across various nation state actors, obviously, there's a level of sophistication and trade craft. And as I pointed out in my testimony, the trade craft and operational security was superb.

One of the things that we typically look for are things like markings within tool chains. And what we saw in particular with the backdoor and the build process was something we call code washing.

That was actually removing these tool chains to -- these fingerprints that Kevin indicated that our company and his company keep on file, right? So, we know who the bad guys are and how they operate.

In this particular case, these tool chains and the infrastructure is very unique. What that means is they took particular care to actually conceal their identity and at the highest level, we've attributed as I said in my written and verbal testimony to a particular cluster of activity.

I know the government has talked about Russia as being one of the threat actors. From our perspective, we have nothing further to add to either confirm or deny that. But what I can tell you, it is absolutely a sophisticated nation state actor.

And as Kevin said, this took a lot of work. A lot of planning went in to this. And when you think of how difficult software is to build. Each one of my esteemed panelists are in the software business.

We know how hard it is to build software, to get software working and the idea to actually inject something and have it all work without errors and without anyone actually seeing it is, again, superb trade craft and something you have to look at and to say it's very novel on its approach.

So, I'll turn it back to Kevin and Brad. They probably have some further thoughts on the attribution piece, but as I mentioned, a sophisticated actor that we continue to track.

MANDIA: And one thing unique to this case is when you do the evidence on a thousand cases a year and something doesn't fall in to a grouping, that's odd, that's peculiar. And then when you go back 17 years of cases and digital fingerprints and it still doesn't fall into it, you start doing the process of elimination.

You talk -- when we found the IP addresses used to attack FireEye, we did go to partners like Microsoft. We went to the U.S. Government, what I call ring zero. You go to the Intel agencies.

Nobody had seen them in use before. I'll just sum up my comments this way. We went through all the forensics. It is not very consistent with cyber espionage from China, North Korea or Iran. And it is most consistent with cyber espionage and behaviors we've seen out of Russia.

WARNER: I appreciate those answers. I do think we've had the previous administration acknowledge likely Russian. We've had testimony of the people in front of us. We've had the current administration acknowledge this source as well.

I think the sooner we make even more fulsome attribution, the better, because we need to call out our adversary. We know who did it and plan an appropriate response. While this incident and I agree with Senator Rubio, we don't even have the language down entirely, sometimes we know what espionage is. We know what denial and service attack would be at the other end of the spectrum where this fits because I think one ongoing question, but I think we've often times talked about this as a SolarWinds hack, but there are other vectors, in my understanding the Wall Street Journal has reported that as many as 30 percent of the victims were not accessed to SolarWinds but by other means.

And maybe this is best for FireEye and CrowdStrike and, obviously, Microsoft would have a view as well. Why aren't we getting more details about the other vectors that the adversary has entered, the other platforms that may have been utilized?

Again, I think this is reflective of the point that since we are totally waiting on willing participants, we could still be uninformed, because other major enterprises could be victims as well, but had not chosen to come forward.

So, how can we get a better handle on the non-SolarWinds component to this attack?

MANDIA: Yes. I can tell you, this is -- we're doing Stage 2 investigations right now for our customers. And the number one other way we're seeing these attackers break in is what's called password spraying.

They're just popping past phrases, they got from some breach over here and they're recognized. If you think about all of us probably have Amazon accounts, we have Microsoft accounts, we have Google, whatever we're using, we have an email account and a pass phrase that we may use to access a whole bunch of applications. Some of those third party breaches make our user ID and pass phrase aware to the threat actor and then they try it on your corporate networks.

When I say password spraying, I almost feel like, "Sir, they know some of these pass phrases by the time they show up and knock on your door." So we have 3,300 employees at FireEye, I have to believe that some of them use their fireeye.com email to access dozens, if not more, the apps on the internet. If any of those vendors get compromised and their pass phrase is compromised and use the same pass phrase in amazon.com as fireeye.com, we may have a problem. So that's another attack that they use.

And here's a reality, this group has zero day capability most likely. How they get initial foothold to a network will continue to change. But the way you know it's them is when they come back in, they target the same things, the same people, the same emails, similar documents, like you have collection requirements.

WARNER: But my question, I want to make sure and Brad and George, if you want to add to this, again, we talked about this as a SolarWinds hack but there are other vectors that they entered.

And for the fact that you came forward for SolarWinds, Microsoft came forward, there may be other very large enterprises that have not been as forward-leaning that may mean this vulnerability still exists.

SMITH: Yes. I would say Mr. Chairman a couple of things. First, absolutely there are more attack vectors and we may never know exactly what the right number is.

I think the first question you're in effect asking is, "Well, why?" And I would analogize to this, this is like finding someone in the building and now you have to figure out how they got in. And in our case at Microsoft, we identified 60 customers where we figured out that they had obtained once they got in, typically the password to somebody, an IT administrator who can get them into, say, something like Office 365. But in each instance, they got in on premise. So it wasn't in our server or our service. And so we need to work with somebody else to get to the bottom of it.

WARNER: But doesn't that mean though that this is not demonstrating a unique vulnerability that's in Microsoft Enterprise software or Microsoft Cloud but there may be other brand name players that may have been penetrated that have not been as forthcoming our leaving policymakers and potentially customers in the dark, is that true or not true?

SMITH: It is absolutely. So I think it means two things, one is, yes, there's a variety of services and there are a lot of ways in. I also would just pick up one of the things Kevin said, because he used a phrase that is familiar to all of us in the cybersecurity community but probably not to, say, somebody who is watching this hearing from home.

This notion of a password spray. I think in recent years we've all sort of learned that people may try to figure out our own individual password, a password spray is when you use a single password and you apply it to a lot of accounts. For example, if I were to go back to where I grew up near Green Bay, Wisconsin and have a thousand email addresses from people in Green Bay and I just applied the password Go Pack Go, I'll bet dollars to donuts there's a Green Bay Packers fan who's using that password. In fact, I'll bet there's more than one.

And if find 10 of those thousand, then I'm in and I can go from there. So it just points to a variety of tactics from the most sophisticated. Really, when you're talking about disrupting a supply chain to the very broad that point to just a lot of factors, we all need to keep learning about to secure our own email and other accounts.

WARNER: Well, I'm going to move to Senator Cornyn but it does beg the question that Senator Rubio and I both asked about when a large enterprise like Amazon is invited, they ought to be participating.

There are other brand name known IT and software and cloud services that may have been vulnerable to this kind of incident as well and their public and active participation, we're going to make sure that takes place. Senator Cornyn.

**CORNYN: Thank you Mr. Chairman and thanks to each of you for testifying here today. I share the concern that has been expressed that Amazon Web Services decline to participate. I think that's a big mistake.**

**It denies us a more complete picture that we might otherwise have and I hope they will reconsider and cooperate with the committee going forward. Mr. Ramakrishna, thank you for talking with me yesterday and since you're headquartered in Austin, Texas, I took particular note of the fact and appreciate that conversation. I think one of the things we discussed is something that Chairman Warner brought up and that is even though SolarWinds is the focus of what we're discussing here today, this is not unique to SolarWinds, correct?**

**RAMAKRISHNA: Senator Cornyn, thank you for that question. You're absolutely right. I'll elaborate on the question that Senator Warner asked and tie the two comments together here.**

**Supply chain attacks are happening as we speak today independent of SolarWinds. There was a report just two days ago about a fence company being hacked and it was dubbed as a supply chain attack. As we discovered what we call Sunspot, the code, the injector tool and as we evaluated it, it is blindingly obvious that that can be applied to any software development process, which is the reason why we believe that dubbing it simply as a SolarWinds hack is doing injustice to the broader software community and giving as a false sense of security possibly.**

**Which is the reason why that even though we are taking corrective steps and learning from this experience, we consider it our obligation to be a very active participant in this endeavor to make us all more safe and secure by promptly outlining our findings and communicating them with both our government authorities as well as the industry.**

**CORNYN: Our time is limited today and I hope at some point we can talk about the attribution and putting the Russian intelligence services or whoever is responsible here at risk because right now it seems to me that we are doing a very bad job generally speaking of punishing the people who are perpetrating these attacks.**

**But let me just ask you, at different times I know there's been legislation offered. Senator Collins and I discussed some that she had introduced previously with Joe Lieberman, our friend, former Senator. It seems to me that there should be an obligation of some sort on the part of a victim of a cyber attack like this to share what they know, what they've learned with the appropriate authorities. And I can only imagine the chills that run up and down some people's backs when I say that.**

Think about liability concerns, other reputational risks and the like. But if we're going to get our arms around this at all, it seems to me we need to know a lot more than we know under the current practices in terms of the obligation of the victims to step forward. Before I ask you about that and what that would look like, perhaps with some sort of liability protection associated with it, I would tell you that I'm a member of the Judiciary Committee as Senator Feinstein is and we actually have designated seats on the Intelligence Committee from certain authorizing committees like the Judiciary Committee.

And Mr. Smith, from your experience testifying there, usually when we're talking about data breaches, people want to talk about the company that allowed the data breach, how can we sue them? And which is an entirely different perspective that I think we need to have a more complete approach to this and one that does not treat the victim as the offender, but one that works more cooperatively.

So what about some sort of mandatory disclosure obligation that maybe would be coupled with some sort of liability protection? I know in the intelligence field in the past, phone companies that have cooperated with certain collection have gotten liability protection as part of that. Mr. Smith, do you have a view on that?

SMITH: Yes, I do. I think the time has come to go in that direction. I think Senator Collins was either ahead of her time or the rest of us were behind our time. But either way, I think we can find a way to move forward this year.

I would perhaps use the word notification rather than disclosure. We should notify someone. We should notify, I think apart of the U.S. government that would be responsible for aggregating threat intelligence and making sure that it is put to good use to protect the country and for that matter, people outside the country. I think we need to decide upon whom that duty should fall, it should certainly fall on those of us in the tech sector who are in the business of providing enterprise and other services.

I think it's not a bad idea to consider some kind of liability protection, it will make people more comfortable with doing this. This is about moving information fast to the right place so it can be put to good use.

CORNYN: Mr. Chairman, can I ask the other witnesses if they have a different view or additional views on that topic?

MANDIA: No, I agree with it and coming down to another level of specificity, to me, notification needs to be confidential or you don't give organizations the capability to prepare for those liabilities.

And so we like the idea of you can notify with threat intelligence that's actionable. You get speed from that if it's confidential. Because you can have threat data today and you're arms around the incident three months from now and it's just too big of a gap to have a disclosure law and we're getting the intel three months to five months too late. So I like the idea of confidential threat intelligence sharing to whatever agency has the means to push that out to places, then disclosures that with legal requirement to inform those who are impacted and you don't know that day one.

And in FireEye's case, we were sharing intel really fast and we did not know what we had lost in our breach yet. But we knew there were something different about it. So I think just an extra detail, get the intel out there quickly if it's confidential.

CORNYN: Mr. Chairman, my time is expired. So I'll yield back and maybe...

WARNER: Well, I think this is a subject we're going to come back around to. And there are models out there. I don't think our traditional reporting mechanisms necessarily work with the National Transportation Safety Border. Senator Wyden is up next.

WYDEN: Thank you, Mr. Chairman. The impression that the American people might get from this hearing is that the hackers are such formidable adversaries that there was nothing that the American government or our biggest tech companies could have done to protect themselves.

My view is that message leads to privacy violating laws and billions of more taxpayer funds for cybersecurity. Now, it might be embarrassing, but the first order of business has to be identifying where well known cybersecurity measures could have mitigated the damage caused by the reach. For example, there are concrete ways for the government to improve its ability to identify hackers without resorting to warrantless monitoring of the domestic internet.

So my first question is about properly configured firewalls. Now the initial malware in SolarWinds Orion software was basically harmless. It was only after that malware called Home that the hackers took control, and this is consistent with what the Internal Revenue Service told me which is while the IRS installed Orion, their server was not connected to the internet and so the malware couldn't communication with the hackers. So this raises the question of why other agencies didn't take steps to stop the malware from calling home.

So my question will be for Mr. Ramakrishna and I indicated to your folks I was going to ask this, you stated that the backdoor only works if Orion had access to the internet which was not required for Orion to operate. In your view, shouldn't government agencies using Orion have installed it on servers that were either completely disconnected from the internet or were behind firewalls that blocked access to the outside world?

RAMAKRISHNA: Thanks for the question Senator Wyden. It is true that the Orion platform software does not need connectivity to the internet for it to perform its regular duties which could be network monitoring, system monitoring, application monitoring on premises of our customers.

WYDEN: Yes. It just seems to me what I'm asking about its network security 101 and any responsible organization wouldn't allow software with this level of access to internal systems to connect to the outside world and you basically said almost the same thing.

My question then for all of you is, the idea that organizations should use firewalls to control what parts of their networks are connected to the outside world is not exactly brand new. NSA recommends that organizations only allow traffic that is required for operational tasks, all other traffic ought to be denied. And NIST, the standards and technology group, recommends that firewall policy should be based on blocking all inbound and outbound traffic with exceptions made for desired traffic.

So I would like to go down the row and ask each one of you for a yes or no answer whether you agree with the firewall advice that would really offer a measure of protection from the NSA and NIST. Just yes or no and I don't have my glasses on, maybe I can't see all the name tags, but let's just go down the row.

MANDIA: And I'm going to give you the, it depends. The bottom line is this, we do over 600 red teams a year, firewalls never stopped one of them A firewall is like having a gate guard outside of New York City apartment building and they can recognize if you live there or not and some attackers are perfectly in disguise as someone who lives in the building and walks right by the gate guard, it's in theory, it's a sound thing but it's academic. In practice, it is operationally cumbersome...

WYDEN: I don't want to use up all my time. We'll say that your response to NSA and the National Institute of Standards is, it depends. Let's just go down the row.

RAMAKRISHNA: So my answer Senator is yes, to standards which is on NIST 800-53 and others define specific guidelines and rules.

WYDEN: Very good.

SMITH: I'm squarely in the it depends camp.

WYDEN: Okay.

SMITH: For the same reasons as Kevin.

WYDEN: Okay. I think we have one other person, don't we?

KURTZ: Yes. And I would say firewalls help but are insufficient. And as Kevin said and I would agree with him, there's a breach that we've investigated that the company didn't have a firewall or even legacy antivirus.

So when you look at the capabilities of a firewall, they're needed, but certainly they're not the be all and end all and generally they're a speed bump on the information superhighway for the bad guys.

WYDEN: I'm going to close and my colleagues are all waiting, the bottom line for me is that multiple agencies were still breached under your watch by hackers exploiting techniques that experts had warned about for years.

So in the days ahead, it's going to be critical that you give this committee assurances that spending billions of dollars more after there weren't steps to prevent disastrous attacks that experts have been warning about was a good investment. So that discussion is something we'll have to continue. Thank you, Mr. Chairman.

WARNER: Senator Cotton on the web.

COTTON: Yes, I am here. So Thank you Mr. Chairman. Gentlemen, thank you for your appearance today. I want to start Mr. Smith with you. Microsoft has said some of its source code was stolen, does that present future security risks? And if so, what are you doing to mitigate it at Microsoft?

SMITH: Well the short story is, our security system does not depend on the secrecy of our source code. I mean we live in a world where probably there's more source code by tech companies published in open source form than there is that's not published.

And at Microsoft, our source code is accessible to every Microsoft employee, it's not considered to be a particular secret. And our entire threat and security model is based on the premise that there will be times when people will have access to source code. Do we like the fact of this after thought? Absolutely not, but we do not believe that it undermines or threatens our ability to keep our customers or ourselves secure. We will by the way, as we always do, to answer the rest of your question senator, we'll ask ourselves what do we change? It's not apparent to me that I need to have access to our source code, it's not apparent to me that our Senate lobbyists need to have access to our source code. So, we may have fewer people that have access to source code in the future but it's really not at all the heart or center of what we're focused on here.

COTTON: Okay. Mr. Ramakrishna, approximately 30 percent of the victims of the attack were not using SolarWinds software. What do you think that tells us about the nature of the attack and what victims were targeted and how they were targeted?

RAMAKRISHNA: Senator Cotton, thanks for the question. This is referring to the Wall Street Journal report, I believe. Thirty percent is an approximation. As best as we know, there are many different types of attacks and different types of threat vectors.

We are not a security company per se, so we wouldn't have detailed information about those types of threat vectors, but what I can share is the discoveries that we have made with Sunspot can apply to any supply chain out there and it's quite possible that there are active supply chain attacks ongoing right now, some of which we may know about, some of which are yet to be discovered.

COTTON: Mr. Mandia or Mr. Kurtz, would you like to respond as well?

MANDIA: George, go ahead.

KURTZ: Well, again, when you look at the supply chain attacks here, it's very difficult obviously to identify these things. And when we look at the adversary's capabilities and we look at what was actually done as we talked about earlier, it's not an easy problem to solve.

And from my perspective, it's one that we have to come together, we have to continue to share intelligence and information and we have to realize that there are many other techniques and actors that are out there, and when you look at the overall landscape, 30 percent weren't from SolarWinds, this isn't a surprise. Over the last year, we stopped 75,000 breaches that were in process and probably a quarter of them were nation states. So this happens every day from every nation state actor, every e-crime actor, and there are variety of tools and different techniques and tasking orders that are out there.

So, it's an ongoing effort and I wish there was a silver bullet, there isn't, but I think a big part of this is exposing the techniques and just how prevalent these attacks are to the American people so that we can do something about it and we can come together as a group both in the technology field as well as in government.

MANDIA: And Senator Cotton, this is Kevin Mandia speaking, to me, the attacker did the SolarWinds implant, they've already moved on to whatever is next. We got to go find it, this attacker, maybe their pencil's down for a few months but the reality is they're going to come back, they're going to be in ever present offense that we have to play defense against and how they break in will always evolve and all we can do is close the window and close the security gap better next time.

COTTON: Okay. And one final question, I think I'll direct this towards Mr. Mandia and Mr. Kurtz again. To what extent do we think this was designed for what we might call collection in the intelligence world? Simply trying to collect information to learn more about America's intentions, plans, capabilities or what you might call a covert action in the intelligence world? Say, sabotage of public utilities or military applications and so forth, or could it be both?

MANDIA: Yes. George, I'll jump first because we got to see what they did firsthand when they broke into us. The reality is this, they were very focused, they had specific individuals that they targeted, they had keyword searches that they did when they broke in.

So this was not a group that operated like a tank through a cornfield. They had a plan, they had collection requirements, and to some extent, I would say they were disciplined and focused on those collection requirements. Not a fishing expedition to just grab whatever they could grab.

KURTZ: And just to add what Kevin says, I think it's important to realize as technology companies, we all leverage big data. The adversary does as well and while they're collecting this information, they're also storing it, they're indexing it and they have the ability to go back to it.

So if a new order comes in, a new specific order to target a company, target a government organization, they can look for that access, they can look at what's already been collected, they could leverage at. The second piece of this is, the early days it was network exploration, then it turned into data exfiltration and then it turned into data destruction and impact, right? So certainly when you have this level of access, you can collect data, if you start impacting systems it's a pretty good way to get caught.

So could it be turned into that? Absolutely. But in general, what we've seen is collection and that simply goes into the big machine, the big apparatus to be used again for further missions.

WARNER: Senator Bennet.

BENNET: Thank you. Thank you all for being here today. Thank you, Mr. Chairman, for holding this hearing. I wanted to get some clarification on the -- on -- along the same lines as Senator Cotton actually. Mr. Mandia, maybe I'll start with you just for people at home who don't understand how -- what -- you know, what they've read is this is a SolarWinds investigation, that's what they imagine we're dealing with here. That's clearly not the case based on what we saw in The Wall Street Journal report with only 30 percent of the folks who somehow got pulled into this had no SolarWinds...

MANDIA: Right.

BENNET: ...connection. Help us understand what that means in terms of the ongoing nature of this -- you know, when you say they put their pencils down, have they really put their pencils down or are they out there working their pencils and we just can't see it because we don't know? You started out at the beginning saying, you know, maybe they went through a list of like five to ten vendors and said, these are the likely ways in and we'll pick this one. But clearly, they picked the other ways in as well. So I just -- I'm just trying to get a sense of the full scope of how...

MANDIA: Yes. And, you know, when I said pencils down, I mean, they were so successful on this breach, they probably got a few days off because they collected so much information.

BENNET: Right. So they're waving the flag.

MANDIA: Well, they're basically -- right now, there's such vigilance in the security community, they're not going to spoil their latest technique right now. We're all looking for it. So they're pencils down for the next great implant.

BENNET: Right.

MANDIA: I would be if I were them. Every intrusion starts with initial access. How an attacker gets that varies. When we say the SolarWinds implant, that was the initial access for a campaign this group did from March of last year till about December last year when we started detecting it. But this group's been around for a decade or more. The -- different people go in and out of that group probably. We're probably responding to the kids of the people I responded to in the '90s when this group was active.

So, the bottom line, how they gained a foothold in the victim network, SolarWinds was a way, they will always have other ways. This is a group that hacks for a living. And then when they break in, what they do after they break in really doesn't change that much. They target specific people, primarily folks -- at least in our case, it did work with the government. They target government projects. They target things that are responsive to keywords.

We respond to a lot of threat groups that when they break in, you can tell they broke in to make money or they broke in and there's a manual review where somebody's literally going through every file alphabetically on a desktop. These folks have economy of movement. If they broke into your machine, sir, they string search it, they find responsive documents, they get out of dodge. They have an economy that shows they're professional and that doesn't change. So if they broke in yesterday via SolarWinds and we patched that and fixed it like we have, tomorrow they're going to have something else, and they're going to try to come back through the, whatever doorway they can find.

BENNET: And tomorrow, they might be looking for something else, too.

MANDIA: The good news is usually they aren't, but you're exactly right, the collection requirements could change. We've identified this group because they'd break into a company and then we can get them out. And if they got back in, they're after the same sort of things. And that's one of the indicators it's still them. So their tools and tactics can change, but a lot of what they target does not.

BENNET: And I'm happy for anybody to jump if you'd like to, but with the rest of my time, there was some discussion earlier -- sorry we're in and out going to votes and things -- about, you know, reasons they might not want to actually destroy data or destroy systems that -- because they might get detected if they do that whereas if they stay in there and they don't mess around with stuff, they -- but if they wanted to -- if they wanted to really do mayhem in our systems, what would that look like? What does our worst nightmare look like? Mr. Smith?

SMITH: Well, I'd offer a few quick thoughts, first building on your -- answering your prior question, then answering this one. I would just add that in addition to, you know, targets in the United States, we have identified targets in Mexico, Canada, the U.K., Belgium, Spain, Israel, and the UAE. So, it was broader and international in scope.

Second, you know, 82 percent of the total 60 targets, victims that we identified were outside government. So I think there's an aspect to your question, well, who else were they targeting and why? And I would say that there are at least two other reasons that we would surmise, two motives, if you will. Sometimes if you're going after a government agency that has very good security practices in place, you might look for a third party that might have an individual who was given password and network access to say the government's network.

And you might hope that that third party organization, maybe it was a computer service provider, maybe it was an accounting or consulting firm, maybe it was a think tank that was working on a contract. You would hope that maybe they have lesser security in place and that's why you would start there. It's a vehicle to get somewhere else. And then I do think at times they target tech companies, in part to understand how technology works, but frankly, it's perhaps in the category of counterintelligence.

Every day, we are looking -- you heard the reference to threat hunting. We are looking for evidence of this organization engaged in attacks. I think they want to know what we know about them and what their methods are. But then I do think your other question is so important, because at the end of the day, what do you do once you're inside? Do you just collect information or do you wreak havoc? Well, this agency typically collects information, but we know exactly what havoc looks like. All you have to do is look at a day in June in 2017 when another part of the Russian government used exactly the same technique, a supply chain disruption with a Ukrainian accounting software program. That, too, was an update.

It turned off, damaged 10 percent of that country's computers. ATMs stopped working, grocery stores stopped the capacity to take credit cards, television news stations went off the air. That is what havoc looks like. And that is what we need to be prepared to defend against as well.

WARNER: We're going to move to Senator Heinrich. That -- Mr. Smith just referenced is what we would refer to as Notpetya potentially existed, even this attack. Senator Heinrich.

HEINRICH: Thank you, Chairman. So if I have this right, a nation-state actor that is in all likelihood the Russians used U.S. software and then command and control servers in U.S. data centers to conduct this attack. And I think the fact that this attack was launched from within the U.S. is potentially a really important part of the story. Advanced persistent threat actors know that the NSA is prohibited from surveilling domestic computer networks. So it makes sense for them to circumvent U.S. surveillance whenever possible. For any of you, do you believe that the adversary launched the attack from U.S. servers in a deliberate effort to avoid surveillance?

SMITH: I think it was sort of an IQ test. We can't know exactly what they thought, but it looks like they passed the IQ test. They figured out that it would be more effective and less likely to be detected if it was launched from a U.S. data center.

HEINRICH: Anyone else want to add to that or in agreement?

RAMAKRISHNA: No, I think I would agree.

MANDIA: I agree with those statements.

RAMAKRISHNA: Yes.

HEINRICH: For Mr. Smith, while the focus continues to be on how the private sector shares information with the government, we also want to ensure that the government is doing enough to share information with the private sector. Mr. Smith, you expressed concerns in a blog following the SolarWinds attack about the federal government's insistence on restricting through its contracts our ability to let even one part of the federal government know what the other part has been attacked. Can you elaborate a little bit about this comment? And in what ways could the Cybersecurity Information Sharing Act of 2015 be improved to ensure that that -- that is possible?

SMITH: Yes, it was, I have to admit, one of the things I found surprising and a bit frustrating for us, because the first thing we do when we identify a customer who's been attacked is we let them know. We notify each and every customer. It was immediately apparent to us that it was important not just to let an individual department or agency of the U.S. government know, but to make sure that there was some central part of the government that would have this information about the government as a whole.

And what we found was that our contracts prohibited us from telling any other part of the U.S. government. So we would basically go to each agency and say, "Can you please tell so and so in this other place," and the good news is people did, they acted quickly, but it does not strike me as the type of practice that makes a lot of sense for the future.

HEINRICH: So probably not -

SMITH: There is an opportunity for reform.

HEINRICH: Probably not the most efficient way to make sure information travels quickly.

SMITH: It doesn't seem like it's consistent with the year 2021 in technology.

HEINRICH: Mr. Mandia, in your statement for the record, you said that victims of crime are the first to know when they've been violated, but in case like this, only a few government agencies and a handful of security or other private companies are in a position to be the first to know. I agree that doesn't seem right. You suggested that a small group of cyber first responders could prevent or mitigate the impact of cyber incidents through sharing information quickly and confidentially. That's a very intriguing idea. How -- can you describe how you think that would work?

**MANDIA: You bet. There's got to be a way for folks who are responding to breaches to share data quickly to protect the nation, protect industries, and that would require A, defining what is a first responder. And I think it's pretty simple. If you're -- if you're trying to figure out what happened to unauthorized or unlawful access to a network, you're a first responder. And if you do that for other companies beside yourself, you're a first responder. And first responders should have an obligation to share threat intelligence to some government agencies so that without worrying about liabilities and disclosures, we're getting intel into people's hands to figure what to do about it.**

**Right now, the unfortunate reality is a lot of times when you share a threat intel, it's just the public disclosure. And it makes people wary to do so and we slow down the process. So that's what I mean by that. I could articulate it more, but first responders know who they are and I think it's easy to define. We have many laws that define certain categories like internet provider. We need to know -- if you're a first responder, you're obligated to get threat intel into the bucket so we can protect the nation.**

**HEINRICH: Oh, I think that's very helpful. When you detected this activity, were you obligated to tell the U.S. government why or why not and was that obligation legal or moral?**

**MANDIA: So we notified the government customers we had before we went public with the breach. And we, you know, we found out later based on contractual reviews who we had to notify or not, but the reality is, the minute we had a breach, I was talking to what I call Ring Zero, the intelligence community, law enforcement, you don't want to get email when you don't know if your email is secure. So the reality is, is I would say on the record, I think we told every government we had that we had a problem, period, before we even went public.**

**WARNER: I think...**

**HEINRICH: Thank you.**

**WARNER: ...Senator Heinrich, both the point that this was launched from domestic servers and the lack of information sharing were really important points. And now, our -- one of our new members joining us remotely, Senator Casey, your first intelligence questions.**

**CASEY: Mr. Chairman, thanks very much and thanks for the welcome to the committee and I appreciate the testimony of our witnesses. I wanted to start with -**

**WARNER: Can you get a little bit closer -- Bob, could you get a little closer to the mic? You're not coming through that well.**

**CASEY: Let me turn that up. You can hear? Okay. I wanted to start with the role of the federal government here and maybe just go down the panel starting with Mr. Mandia to give us an assessment of the federal government's response to date and then I'll move to a second question regarding what we do going forward. So, Mr. Mandia, why don't we start with you?**

MANDIA: Yes, I think without a doubt, the number one thing the federal government can do that the private sector cannot do is impose risk and repercussions to the adversaries, period. So we got to have some kind of public doctrine to Mr. Smith's idea of rules of the road. We got to communicate where's the red line. I know we think it's a tough thing to define and we admire the problem, but we got to come up with what's tolerable, not tolerable, communicate it so we don't see gradual escalation.

But to impose risk and repercussions is the purview of the government, and the second biggest thing is the attribution. The government's in the best place to get attribution the most right, so those two things. And by the way, there is no risk and repercussions if you don't know who did it. So those are the two things that I'd firmly place into the government is best suited to do that, and I'll leave it to some of the other witnesses on the government's role on how to safeguard the private sector and we're with the private sector because I know we have a lot of great ideas.

RAMAKRISHNA: Senator, I'll keep it quick and the suggestion that I would make is to leverage some of the recommendations in the Solarium Commission report and have a single entity in the government, that public sector entity where all private sector entities can go and communicate with and communicate to, and have the responsibility of that agency to then disseminate it to every relevant party. To date, we feel like we have to communicate with multiple agencies and sometimes that doesn't help us from a speed and agility perspective.

SMITH: Let me, if I could, point to two successes that I think are worth building on. First, I think it's really notable that the NSA in December published a circular that described in technical detail the nature of the attack how people could identify whether they were victimized by it, and how they could protect themselves from it. And I think that it was extremely well done from a technical and cybersecurity perspective and it was published to the world. And I think that the NSA and the U.S. government did the world a great service. And that's the kind of thing that we should aspire to have our government do in the future.

Second, last week, I thought Anne Neuberger at the White House in a press conference took a similarly critical step. She shared to -- for all of us, you know, information that frankly none of us had, namely that the government had identified roughly a hundred private companies and nine federal agencies that had been impacted by this incident. And that tells me that there is now at work real efforts to consolidate this information across the different parts of the government, so that's encouraging. She's also indicated that her work is far from done. They're focused on next steps that need to be taken in a variety of ways.

But I do think this is a very important moment. The government can do -- can speak authoritatively about the nature of attacks and how to protect ourselves and the government can speak authoritatively about the scope that it has happened.

KURTZ: I would also -- just to jump on this, I would also say that CISA's done a lot of work here, a lot of great work, had put out some I think interesting information, indicators, some scripts that helped the public. And while we're talking about the government, we're talking about corporations, there's a whole host of smaller entities that are out there that have no real way to protect themselves.

So I think to Kevin's point as a first responder, which we are, which he is and others, it's important that we have a single source that we can go to. We're doing incident response not only for big companies and governments, but for many small companies. We need to be able to share this information as quickly as we can without impacting the customer themselves.

CASEY: Mr. Kurtz, I'll end with you just with one follow-up. The -- when you go through what I think were six proposals or recommendations, what do you think is the most urgent at least as it relates to the federal government?

KURTZ: Well, I think there's probably a couple things, but certainly, threat hunting is one of the biggest areas and as we've talked about before, it's a sophisticated actor. With enough time and effort, they're going to go get in somewhere. We always make the distinction between an incident and a breach. There isn't a major company or government on this planet that hasn't had an incident. And they will continue to have incidents, but you want to be able to identify those very quickly so they don't turn into breaches.

And these are like sentries that are looking for the bad guys. They're looking for these indicators. They're looking for these back doors. And it's a tall task. I pointed out things like machine learning and artificial intelligence. All my fellow witnesses are working on these sort of techniques as well as, and that's a big part of go-forward strategy. Figure out what's there, use the technology to our advantage.

WARNER: Senator Burr.

CASEY: Thanks very much. Thanks, Mr. Chairman.

WARNER: Thank you.

BURR: Let me thank all of our panelists today for your willingness to be here and more importantly, for your knowledge in this. I've got to reflect for just a minute and I'm going to do it even though Senator Wyden left because I strongly disagree with what he implied. He implied that because NSA and NIST said that proper hygiene is a firewall, that that should be something that should be mandated and everybody should use it and that would solve our problem. And the three of you that deal specifically in searching out intrusions said, no, no, no, no. It's helpful, it doesn't solve it.

And to suggest that in the day of COVID that you've got a choice between washing your hands, hand sanitizers, masks, but if you choose just to wash your hand and not do the other two, you're never going to get COVID. It's ludicrous. And I want the record to show that what the response from the who track these was, listen, this is sophisticated. They're way past this. So yes, that's a good thing for companies to adhere to, but don't think that that's going to solve it with the adversaries we're up against right now.

I want to turn to George just real quick and I want to go on Senator Heinrich's question. In the SolarWinds attack, Amazon Web Services hosted most of the secondary command and control nodes and all of AWS's infrastructure was inside the United States. Now, I feel like having a cyberattack deja vu here, whether it's Russian hack of DNC in 2016, the North Korean Sony hack, or current supply chain hacks, we constantly see foreign actors exploiting domestic infrastructure for the command and control to hide the nefarious traffic in legitimate traffic.

Here's the problem. Given the legal restrictions on the intelligence community, we don't have the ability to surveil the domestic infrastructure, so what should the U.S. government role be in identifying these types of attacks?

KURTZ: Well, I think it's working with providers like AWS, working with folks like Microsoft, working with others, CrowdStrike, and FireEye, and others, because when you look at this particular attack, why did they use U.S. infrastructure, because they just wanted to blend in, right? And I can tell you there's a ton of attacks that we look at that use foreign infrastructure, that use bulletproof hosting which is the ability to anonymize and pay for hosting and infrastructure, and we know who they are and we tend to look for those bad actors.

Right? So if you can use infrastructure that looks legitimate no matter whose infrastructure it is, you're going to blend in and make it harder. And this particular attack was insidious just the way it communicated and the protocols it used, it looked like legitimate traffic going to infrastructure that is normal. But that's why it's important when you think about these attacks to have visibility. I talked about threat hunting, to have visibility on the end points, because that's the tip of spear. And these network access devices are just speed bumps as I talked about earlier. What's actually happening is on the endpoint, what's actually happening is beaconing out, and you have to have visibility. And you have to collaboratively work with the private sector and the public sector together. And I think that's the only way we're going to solve it.

BURR: Kevin, I want to turn to you and I want to ask for a little more specific statement. You alluded to the fact that this is not going to stop without government dictate that says here's what we're going to do. Let me just ask it this way. Will it stop if they pay no price for what they do?

MANDIA: No, I think if you don't impose risks and repercussions, we're all -- you know, I've used this analogy for so long you'll get how long I've used it. We're all playing goalie and we're taking slapshots from Wayne Gretzy. I mean, the puck's going to get in the net sooner or later. And that's what's happening in cyberspace right now. Folks are taking slapshots and literally, there is no risk or repercussion to the folks doing it. So, we're all fighting a losing battle over time.

BURR: So, Sudhakar, as it relates to SolarWinds, can you build software today without the risk of what happened?

RAMAKRISHNA: Thanks for the question, Senator. The -- we've done extensive analysis with our partners at CrowdStrike and KPMG of our entire build environment and entire infrastructure. And we see no evidence of the threat actor in our environment or in our build systems and our products. We've also learned from this experience and applied them to what I've been describing as secure by design.

One of the key tenets of that is to evolve software development cycles to secure development life cycles. And related to that, we've come up with a methodology where source code doesn't get built in traditional ways and we use parallel build systems with different people accessing them with different access types. And we correlate the output of them across those three to significantly reduce the potential for a threat actor to consistently compromise every one of our build systems at the same time. That is the level of effort our teams are going through to build safe and secure solutions, which I hope will be a model for others.

BURR: Are these practices that you're sharing with others in the industry?

RAMAKRISHNA: We are completely committed to doing it and we're doing it as we do it.

BURR: Thank you, Mr. Chairman.

WARNER: I would simply want to quick comment that I agree with my friend, Senator Burr's comment that a firewall alone cannot keep out a sophisticated actor, but it doesn't mean the corollary, and I had conversations with the CEO of SolarWinds on this, that just because it's a sophisticated actor then means -- that means that you shouldn't do good cyber hygiene.

RAMAKRISHNA: Absolutely.

WARNER: It is not an either/or.

BURR: I agree with you totally. I think what we're hearing and maybe we're just not saying it right is that even with the best cyber hygiene, even with the best protocols in place, because of how good and persistent and how much money a nation-state has like Russia, we're susceptible.

RAMAKRISHNA: Yes.

BURR: It -- you know, the puck is going to get in the goal as Kevin said. And if we've missed anything and you've got something that assures us the puck won't get in the goal, then here or privately share what it is so that we can begin to pursue and flesh out that type of policy.

WARNER: But the problem is we may not know the puck was even in the goal, but if you've got good cyber hygiene, chances are you will discover the puck at some point. We'll continue that hockey analogy now as we move to our next new committee member. Senator Gillibrand, welcome to the committee, and your intelligence committee questions.

GILLIBRAND: Thank you, Mr. Chairman. I want to follow up on knowing whether you've had the puck into the goal. One of you said that the hack that shut down CrowdStrike and other defense software, it affected them before they could start working. So, why did these programs -- why was there no alarm and how were they shut down? And related, why were there no alarms in the SolarWinds and anti-virus software logs which should have shown the unusual behavior access or other traces of unauthorized access?

KURTZ: Yes. So, this is George. Maybe I can -- I can take that. There were probably multiple dozens software technologies that were targeted to actually be shut down. In our particular case, you can think about the camera. You know, if someone came up to a camera and smashed the camera, you'd actually see what they did. And our particular software has a level of monitoring where if someone tries to tamper with it, we would actually be able to see that. And in fact, you'd actually have to reboot the system. As Kevin mentioned, pretty persistent where it waited and kind of did things, you know, overnight...

GILLIBRAND: Yhere was nothing -- there was no alarm even the -- after the 11 days?

KURTZ: Well, once you have admin access on a particular system, if you're shutting it down, you can pretty much do anything you want on it. And that's just sort of a function of how the operating system works. And what we focus on is -- and I talked about this in my written testimony, no silent failure. And we've designed our system that even if there's a failure somewhere along what we call the kill chain, this attack sequence, we're still going to detect something down the road.

And I think this is really important when I talked about threat hunting. You may not catch the initial stage of the attack, but you're looking to catch it along the way and you're looking to do that with speed. If someone's going to rob a bank, there's only so many ways to rob a bank. You've got to get there, you've got to get the money, and have to get out, right? What car they drive, what weapon they use, how they do it, it doesn't really matter.

So, as long as you can identify the chain of activity which is really important, you can stop these breaches and that's why we stopped over 75,000 breaches just last year. So it's obviously a challenging problem, but that's why when we look at this, it's really about risk mitigation using multiple technologies and having visibility across your network.

GILLIBRAND: Right. Mr. Smith, I think you said on 60 Minutes that there were more than a thousand developers working on writing this malicious code. Why do you know that or how do you know that? And with a group that big if it is based in Russia, how we come we didn't detect it or see it before?

SMITH: Well, there was a lot more than a single piece of malicious code that was written. And so one of the things we analyzed what was -- is -- what was done from an engineering perspective on each of the second stage attacks that Kevin was talking about before.

And in essence, what we saw was a very elaborate and patient and persistent set of work. You know, they entered, they -- then as they were in through that back door, they in effect opened a window, they then swept up behind themselves, they closed the back door. They used that window. They identified accounts. They were able, for the most part, to really rely on stealing passwords and accessing credentials especially where credentials were not well-secured, meaning they weren't stored on a hardware dongle or they weren't stored in the cloud, but they were able to get people's passwords.

They were then very persistent in using that -- what we call elevated network privilege to work across a network and just were able to look to look at our estimate of how much work went into each of these individual attacks, how many attacks there appeared to be in total. And we asked our engineering teams, these threat hunters that you were hearing about before, you know, what do you think is on the other side of this? And that was their estimate and we have asked around with others, does this estimate seem off base, and no one has suggested it is.

GILLIBRAND: Let me ask Mr. Ramakrishna a final question. So, the Wall Street Journal reported that there was as many as a third of the victims were accessed by means other than SolarWinds. However, those access vectors including TTPs and infrastructure have not been made public. Why is that and do you expect to release the full details of the other access vectors? And what other ways did the cyber actors use to gain access to victims?

RAMAKRISHNA: Senator, that's a very good question. We, as a manufacturer or producer of IT management tools, do not have the security capabilities to be able to investigate other threat vectors and that's where the colleagues at this witness table with me will be able to help us and the broader industry identify those threat vectors.

On our part, what we have committed to doing and continue to do is sharing everything that we are finding and the significant discovery that I mentioned about Sunspot is one key element of eliminating threat vectors, as we learn some new vectors ourselves as SolarWinds, we are committed to sharing those, but I think the broader security industry will take the mantle on that.

WARNER: Senator Collins.

GILLIBRAND: Thank you, Mr. Chairman.

WARNER: Thank you.

COLLINS: Thank you, Mr. Chairman. Mr. Chairman, let me echo the concerns that Senator Cornyn and you have raised about Amazon not being present. I think they have an obligation to cooperate with this inquiry and I hope they will voluntarily do so. If they don't, I think we should look at next steps.

I also want to thank both of you for mentioning a legislation that Senator Joe Lieberman and I authored and brought to the Senate floor back in 2012 which was defeated largely due to the lobbying efforts of a large business group. And the irony is that this business group at the time that they were lobbying against mandatory reporting was itself being hacked, which it found out about from the FBI later.

I take no pleasure in that. I think that shows how widespread this problem is. I want to follow up on two issues. One is the issue of reporting. Mr. Mandia, we know from the White House's report and from our own briefings that the hackers did gain access to at least nine federal agency networks, yet the United States government learned of this cyberattack through FireEye. So, in your judgment, is it reasonable for us to assume that our government probably would still be in the dark about the Russians or whoever the hackers were, likely the Russians, being on our systems if it were not for your voluntary disclosure?

MANDIA: I think over time I believe we would have uncovered this. I think there's a lot of activity that, out of context, nobody could put their finger on the larger problem. The minute we found the implant and the minute we disclosed what had happened, it connected a lot of dots for a lot of folks. All I can tell you is when I spoke to the government about this, you know, basically as it was unfolding for us, nobody was surprised to what I was telling them. So I think we could sense there was behavior on certain networks that wasn't right, but we couldn't find the cause till we put it all together.

COLLINS: But none of those agencies had taken actions until you contacted them, is that accurate?

MANDIA: I don't know what actions they may or may not have taken.

COLLINS: The second issue that I want to talk about is our critical infrastructure. Eighty-five percent of the critical infrastructure in this country is owned by the private sector and that's one reason that I think mandatory reporting is so critical. We have only to look at what happened in Texas from natural causes to imagine the damage that could be done by a cyberattack. Now, it's my understanding that our government has assessed that this operation focused on stealing rather than taking down networks. But how difficult -- and I would like to ask the entire panel this -- how difficult would it have been for the hackers to disrupt these networks if it wanted to? Why don't we start with you, Mr. Mandia, and just go down the panel?

MANDIA: Two comments, ma'am, very quickly on that. Disruption would have been easier than what they did. They had focused, disciplined data theft. It's easier to just delete everything and blunt force trauma and see what happens, which other actors have done, but what I've observed this group do, and I think this is important detail, a lot of times when you break into a network, you get what's called the domain admin account and just use that to grab everything. It's the key to everything. It's the master key in the hotel.

What this group actually did is they wanted to break into Room 404, they got a room key that only worked for Room 404, and they got the room key for 407. They actually did more work than what it would've taken to go disruptive. But obviously, they had the access required and the capability required should they have wanted to be disruptive to have done so.

COLLINS: Thank you.

RAMAKRISHNA: Senator Collins, I would agree with that based on my studies and research of other similar breaches in other countries such as in Ukraine.

COLLINS: Thank you. Mr. Smith?

SMITH: I would agree as well and I'll just highlight a couple of aspects that I think are important. First, especially when we're talking about publicly-owned critical infrastructure in this country, a lot of it is too old. It needs to be modernized. And I'll just point to one example, one -- some of our work with the state agency responsible for public health, when our consultants went into work with them, they found that the manual for the software was more than 20 years old, meaning the software itself was more than 20 years old.

So -- and that's why you see these ransomware attacks which need to connect with this, they so often target municipalities. We've seen Baltimore. We've seen New Orleans. They target hospitals. So that is in critical need of improvement. I do think the other thing that is really worth thinking about more broadly for the whole committee is I don't think we can secure the country without investing in more cybersecurity people for the country.

There's really a critical shortage nationwide of cybersecurity professionals and I think we could put our community and technical colleges to work in part to get more people into public agencies, into small businesses and others. We are doing a lot to try to publish information. At Microsoft, we have published 31 blogs since we learned about SolarWinds from FireEye, but there's just not enough people in many places to read them and act on them.

COLLINS: Thank you. I know my time has expired, maybe Mr. Kurtz could respond for the record.

KURTZ: Sure. Thank you.

WARNER: I'll just simply mention as well, Senator Collins. You appropriately pointed out the failure to report on the private sector side. There's no obligation on the public sector side.

COLLINS: Right. Well, part of the problem is there should be this exchange of information that's not occurring now on either side.

WARNER: Absolutely. Senator Blunt.

BLUNT: Thank you, Chairman. Mr. Mandia, did you feel when you found this problem in your system, did you think there was a legal obligation to report it to anybody?

MANDIA: We had third party counsel involved. We did not have a legal requirement at least based on the legal advice that I got to disclose at the time that we did. So we did so based on we're a security company, we work to a higher order. Yes, it's all build on trust and you got to report.

BLUNT: And, Mr. Ramakrishna, what -- did you think there was a legal obligation to report this when you found out about it? To the government or anybody else?

RAMAKRISHNA: Senator, I was not with the company when this particular incident happened, so...

BLUNT: Got it.

RAMAKRISHNA: ...I will take it on record and come back to you with exactly what happened at that point in time.

BLUNT: And, Mr. Smith, from your testimony, I think it was point four in your things we should do, though there was some element of it in point three. It's your view that there should be a requirement now that these kinds of things be reported, is that right?

SMITH: Yes, and I think we should build on the conversation we had here, but, you know, we too concluded we had no legal obligation to report, but I think we had a duty nonetheless, first of all, to each customer, second of all, to the U.S. government, and third of all, to the public which is why we published 31 blogs.

BLUNT: So do you think we should -- do you think we should create a legal obligation for you to report if you're aware of a problem like this?

SMITH: I do. I think we need to be thoughtful, tailor it, make it confidential, but we -- we will not secure this country without that kind of sharing.\

BLUNT: So on that topic and we'll just stay with you and then work our way back down. On that topic, these companies, all four of the people represented here have great expertise and great resources which I'm sure you've used a lot of to

figure out how they got there, if you've figured that out, how long they have been there. How would we expect a normal person that does business with your companies to be able to do that on their own.

And maybe Mr. Smith that goes to your view. We need more cyber expertise. But how would we expect a regular company unlike these companies at the table today to have any sense whether anybody was in their system or not?

SMITH: Well, first thing I would say is i think that it is a decision for you to make as to whom you want this obligation to apply. Certainly, it should apply to tech companies. Should it apply to every customer of a tech company? I think that is a separate question.

Second, of course people cannot report something they are not aware of. Our customers who use our cloud services know when we are able to detect that they are being breached in the cloud or they are being attacked, because we tell them. And so, we let them know.

Now, ironically one of the episodes we've learned from this time was in some instances we called people on the phone and we said we're from Microsoft and we want you to know you're being attacked and they're like, yeah, right, and they hung up. They didn't believe that this big company was calling this small business. But that is our job, or responsibility, I think to help our customers and we can provide information to the government or in certain instances, others could as well.

Are you going to ask every small business to do that? It is probably not necessary.

BLUNT: I think if we move forward on that discussion, some helpful thoughts from all of you about when that obligation to report if you have called a customer and said you've been hacked, is there an obligation you should have then to report, we could work on that.

Mr. Mandia, how long do you think this had been in your system whenever you found it? And I know it was the two telephone verification, seeing that extra verifier in there that was the tipoff. How long do you think it had been there?

MANDIA: Well, a couple ways to answer that. The bottom line is a couple months from initial access. But the attacker wasn't live every single day. I think in other words they were on our system for maybe three hours in one day, a week would go by, a couple of hours on another day. We weren't a full-time job for the intruders that broke into us, because they had broken into 60 plus other organizations, if not 100, so we did get their attention, and there are several days of activities before we detected them. But over time, it was several months.

BLUNT: And of course you'd contend that very few companies would be better prepared than yours to find out if somebody is in your system, because that is what you do.

MANDIA: Right.

BLUNT: Mr. Kurtz, you mentioned on the bank robbery example, I think it was something like you get there, you get in, you get the money, you get out. It seems to me that in this intrusion, they weren't all that interested in getting out. What do you think that means, that they would get there and just hang around as Mr. Mandia said, and do something and a week later might do something else? What kind -- what kind of hacker is that? What are they positioning themselves to do? Clearly not to shut down your system at that moment, but why do you think they were persistent in this, what I think is a relatively different way than we might have anticipated?

KURTZ: Well, this is indicative of a nation state actor and it is in their interest to maintain persistence. If they were collecting data, they want to continue to collect information over a period of time. If the campaign as was pointed out, this is the way it works, or you've got different mission objectives and campaigns. If the campaign is over, they certainly would want to remove their tools so they weren't found by companies like CrowdStrike, and FireEye, and Microsoft and others. So it is in their best interest to maintain their persistence because you never know what they are going to need.

And one of the things that I really to want to point out and how this works in practice is that when you get into a system, when an adversary gets in, they don't necessarily know what they are going to find. And then they find some interesting tools, they find some emails that may lead them to another company they can compromise and it's is a massive spider web of interrelated entities and information that they have to collect.

And when you draw that out, if you can imagine a crime scene where you kind of put everything on the bulletin board and you start connecting the dots between the actors that is what it is like for the victims, and from one company to the next company, to the next company, to the next company, to a government agency, they can all be connected together with some of these campaigns. And there is no reason for them to get out unless that campaign is over. And certainly unless they want to remove that Malware and their tools which we've seen in this particular case, because they didn't want anyone else to find them.

WARNER: Senator King?

BLUNT: Thank you. Thank you, Mr. Chairman.

KING: Thank you, Mr. Chairman.

Excellent, excellent hearing, a lot of important points. A couple I just, I want to emphasize.

Mr. Mandia, I will give you another analogy to use, as well as Wayne Gretzky, and that is if all we ever did was lock our windows and robbers never had to worry about going to jail, there would be a lot more robbers. I think deterrence is one of the most important parts of a national strategy and frankly it's one that really hasn't been very well developed in this country. And as you pointed out, I think it has to be declared. It has to be public. The adversary has to know what the capabilities are and that costs will be imposed.

That leads me to a second point that I think Brad Smith mentioned but we didn't really develop, and that is the importance of internationalizing this problem, and that is working with our allies because we're not the only ones -- I think you mentioned there was an attack on a French company by this same group, and to the extent that we have the international community and the establishment of some kind of international norms, red lines, guardrails, whatever you want to call them, then things like sanctions are much more effective. I want the hackers to not be able to go to Monte Carlo as well as Miami, so deterrence is key, and the international piece of it is also important.

And then the final thing that I think has come out today and very clearly is the importance of some kind of joint collaborative environment where there can be an easy and quick and efficient flow of information, liability protection may be necessary, anonymyzing the data may be necessary, but some kind of mandatory breach notification is also part of this package, all of these bills, all of these ideas by the way are part of the work that we'll be doing on the Solarium this year and I look forward to working with the members of this committee on things like the collaborative environment, breach notification, the international aspect of it.

Let me ask a specific question. Mr. Mandia, do we need a central federal attribution office? It strikes me that attribution, the FBI has a piece of it, the NSA has a piece of it, maybe the CIA and somewhere else, attribution is key, you can't do deterrence, you can't respond unless you have attribution. Should there be a central attribution department, if you will, that could act quickly and do attribution more efficiently than is the case today?

MANDIA: I can say this, sir, I don't know if it needs to be a single committee or single agency, but attribution is critical. And any time I get to advise a head of state, it is very simple, if you don't know who did it, you can't do anything about it, so I would argue it is one of the most critical issues we have to solve as a nation is we got to know who did every breach.

I think that those data points will automatically come from multiple agencies with multiple missions, and areas of responsibility and then bring it to the domestic challenges like the SolarWinds breach and all the liability sitting in companies. It is helpful and maybe it's just -- maybe it is the FBI but it is helpful that most organizations recognize that we are expected to defend ourselves from the drive-by shootings on the information highway, but we shouldn't have to defend ourselves from the SVR. I mean that doesn't seem like a benchmark that this nation should set for every small and medium-sized company out there, that you need to defend yourself from a foreign intelligence source trying to hack you.

So I would say this, categorical attribution for these companies that do disclose is very helpful for those companies. So in other words, if there is public attribution that said SolarWinds was compromised by a nation state, good enough, because it takes the wind out of the sails of all the plaintiff lawsuits that we all get when we get compromised and we tell the world about it. Thank you.

KING: Thank you, and it seems to me that moving on from -- clearly we have to do attribution better. The other piece that has come out today, and Mr. Burr, Senator Burr mentioned this, is gaps in our authority. The NSA and the CIA cannot spy on Americans. They cannot watch what is going on in American networks. That sort of leaves the FBI which is really a law enforcement agency as the intelligence agency for domestic cyber attacks. It seems to me that we need to think of how these authorities fit together and what the gaps are to be sure that we have the tools to protect ourselves. Not that we want to spy on Americans, but we also want to be able to protect Americans.

Mr. Mandia, your thoughts on that?

MANDIA: I do believe there's got to be a way for the U.S. government when we need to mobilize, to understand how we can do domestically. And the example I've always used there is very simple if the intelligence community recognizes that there will be an attack on Wilkes-Barre Hospital this Friday by the best hacking group on the planet, we just start moving the patients out of hospital. And that seems like we can do better than that as a nation. We ought to be able to impose the risk profiles that we need to and project our capability domestically when we need to. And right now, I don't see the ability to do that.

KING: I appreciate it.

WARNER: Senator Feinstein? Dianne?

FEINSTEIN: Thank you very much, Mr. Chairman.

I'm looking at this worldwide threat assessment of the United States intelligence community. it was done by Dan Coats, former colleague of ours when he was director of National Intelligence, and it's deeply concerning to me because it points out really the seriousness of this thing and the impact of it. The length of time, eight months, that it went on, nine federal departments, over 100 companies and we don't know, at least I don't, what the Russians took. And it seems to me to have this kind of situation out there, and I've been on this committee for a long time, and not -- and just have a hearing and not do anything about it and know that we know now that there is this kind of vulnerability available.

So let me begin with you, Mr. Mandia, you're a Californian. What do you advise this Senate to do about this?

MANDIA: Yes, there are several recommendations. I still believe it is critical we find a way to have a centralized agency that we can report threat intelligence to, confidentially, and that if you are designated as a first responder in cyberspace, whether private or public sector, you report to that agency. That means we get the intelligence into the hands of people that can take actionable steps way faster than disclosure of incidents which just takes too long.

To Brad Smith's point, and you have -- there are six bullet points, I think it is actually five bullet points and they are all right, and it's what we should do. I'm specifically talking about the threat intelligence sharing. Let's up it a notch. Let's say you have to if you are a first responder.

FEINSTEIN: How would you do that, when you say up it a notch, what specifically would you do?

MANDIA: Have legislation that defines who a first responder is, that if you respond to unlawful, unacceptable or unauthorized access to networks as a business and you see certain things, that threat intelligence -- and we know what it is in the community, it needs to be shared with a specific agency, confidentially shared so you don't have to know who the victims are because the victims have liabilities that make them delay. They will did months of investigation before they would disclose everything. But we want to get the intel faster and into the hands of the right people more quickly. I do believe it needs to be a central agency inside the government. You can't go to three or four, you have to pick one and that if we're responding, we got to let you know here's what is going on.

FEINSTEIN: And this would be private sector as well as government sector?

MANDIA: Yes.

FEINSTEIN: So it would be a comprehensive bill that essentially would set a kind of operational protocol that has to be followed.

MANDIA: It's similar to, there are operating agreements to all the folks who accept credit card use, the VISA operating agreements. You literally have 24 hours to start sharing information regardless once you know. And it's not based on all the things that you may have lost. You've got to get the intel into the hands of the folks that can start safe guarding the nation far faster than what we're doing today.

FEINSTEIN: Could I ask the other two witnesses to reflect on what Mr. Mandia has said?

RAMAKRISHNA: Senator, I agree with the single agency to report to and the public/private partnership. Clearly that is one of our recommendations as well. And that will be consistent with the goal of having speed and agility in responding to these types of events. As you noted, some of these have gone for too long and we've lost time in detecting the perpetrators and taking corrective steps

Additionally, I would recommend in the context of public and private partnerships standards such as NIST and procedures such as CMMC can be included with better collaboration, better transparency between private and public to evolve those from what are today compliance-based methodologies, to focusing on excellence. That is where I think Brad's idea of having a larger pool of STEM. based focused education as well as specific cybersecurity education will come in handy.

FEINSTEIN: Thank you.

RAMAKRISHNA: And then the last thing I would say in the context of coming out and identifying breaches, and encouraging people even to come out and identifying the breaches, there was a concept of liability protection that was discussed. There is significant brand reputation that people are worried about as well. And in the context of this broader work, I'd recommend that we address those as well which are not strictly liability but broader than that.

FEINSTEIN: Thank you. Mr. Smith?

SMITH: Yes. I would endorse everything that you just heard. I would add in the areas of rules of the road, I think that there are three areas that are just clearly ripe for this committee and others to say they are off-limits. The patching and updating of software should be off-limits certainly within...

FEINSTEIN: Wait, the patching and off...

SMITH: And updating.

FEINSTEIN: Updating...

SMITH: Yes.

FEINSTEIN: ...a software.

SMITH: Yes. That would...

FEINSTEIN: ...should be off-limits to whom?

SMITH: For these types of nation state attacks. That would be the first thing. The second would be Cyber attacks on hospitals and health care providers, vaccine distributors. I mean there has been a ground swell about concerted -- over what we've seen in the last year and attacks on that sector.

And the third is attacks on our electoral infrastructure, on voting, on the tabulation of votes, on voter registration rolls. And I think there is a ready vehicle that is ripe because 75 governments but not our own have already signed the Paris call on trust and security in cyberspace, more than 1,000 private organizations including my own has signed that. And I hope that this White House and this State Department will act on that. The consensus is there if U.S. leadership can help push it across the finish line.

FEINSTEIN: Mr. Mandia, would you just reflect for a moment -- just one question?

WARNER: Yes, we've gone through the five minutes.

FEINSTEIN: Okay. Thank you.

WARNER: Senator Sasse?

SASSE: Thank you. Chairman. And thank you to all four of you for being here. This has been a very constructive hearing. I would just associate myself with many comments of folks expressing frustration that Amazon isn't here. I think that they should be and I think we should pursue whatever is necessary. hopefully they will do that voluntarily.

I'd also like to underscore a few things that were said along the way by Angus King about some of the deterrents objectives of the Cyber Solarium Commission. He and Mike Gallagher, a House member from Wisconsin have invested tons of time. I was a commissioner, but those two guys co-chaired it. There is a whole bunch of work to be done about breach notification that they've been taking on in addition to some of the work that Susan Collins has done.

Mr. Mandia, I know you answered it multiple times through the course of the last three, but your summary five minutes ago about the need for a central single repository at the federal government for these breach notifications I think was very succinct and compelling, so thank you for that.

Mr. Smith, when I came back from voting a while ago I think I heard you say, I was just walking into the room that you thought that there were 1,000 highly trained engineers involved in planning this attack. Did I hear you right?

SMITH: That was our best estimate, yes.

SASSE: And could you kind of give us a level set of other attacks or espionage efforts in the past like, say, the CCP's OPM hack, do you have any theory of how many people would have been involved in that, trained folks?

SMITH: Well, I don't, but you certainly didn't need an engineering group of similar magnitude to steal data. You really needed them to think about how to use that data, which is probably some combination of engineering and artificial intelligence. And I do think as we scan the horizon around the world, we are seeing variation in tactics, we are seeing in one part of the world more of this, I'll call it, engineering intensive effort to penetrate individual organizations with great patience and persistence and then extract data on an ongoing basis, as you would if you are a foreign intelligence agency.

In another part of the world, you're probably seeing more collection of very large data sets. and in all probability the way one would make use of those data sets is to aggregate them and use artificial intelligence machine learning to start to knit them together and then, say, use them for disinformation. And so, as we look at the world, we have espionage threats, we have disinformation threats, and then ultimately we always have the threat we were talking about before, of actually damaging a society or a country as we saw in Ukraine.

SASSE: Right. Very helpful. Is there any equivalent breaches that you can think of that would have had this scale of human capital involved in planning them?

SMITH: I can't think of a similar operation that we have seen that would have similar human scale, no.

SASSE: So, this is arguably the largest planned cyber attack ever.

SMITH: I haven't seen anything larger. I think we were having a good conversation before about what label precisely to attach to this. But it was a very -- it's the largest and most sophisticated operation of this sort that we've seen.

SASSE: So, going back to some of Martin Heinrich's questioning and then Senator Burr's follow-up on the same thought, it would be useful for those of us who are not technologists to hear the three of you kind of talk about the difference between the design flaws -- not that anybody is particularly responsible inside the U.S. government for having failed to detect this because it's a new kind of attack, but design versus execution flaws.

Given Martin's points about the NSA being prohibited from surveilling domestic systems, who should, in our current structure, have found this earlier? Again I'm not looking at you to blame cast. I'm looking at us as Congress to recognize that we have an IC that is not structurally prepared to respond to something like this when your greatest capabilities are at the NSA and they're prohibited from the surveilling the systems where they would detect it. The FBI is chiefly responsible for law enforcement investigations after the fact, structurally, we're not prepared to defend against this, are we?

MANDIA: I guess I'll jump in on that one. There's no question you have to have private and public partnership in it, period when you'll get critical infrastructure and who's running it. I want to be clear though, why people didn't detect this, the Achilles heel, is because the door was locked so the attackers had to break into SolarWinds, implant something, we still don't know how they broke into SolarWinds that I am aware of, and this is probably the last avenue in cybersecurity now that we know you've got to worry about supply chain risk, and you are going to see the elevation and security there.

So the reason that everybody didn't detect this right away is over the last 30 years in cybersecurity you used to be able to drive in the front door. And we kind of we closed that. And then it became spear phishing and tailored attacks against individuals and we got really good at that. And now went to the supply chain, and it was inevitable, we knew that they'd get there. Apparently it takes something like this for us to really decide to up the game.

SASSE: But if we think about how many questions you've had to answer today about reporting requirements, you also had a sense, Mr. Smith, you said something about the reporting prohibition ongoing from one government agency to the next. How long was that delay if our structure? If you had been able to notify everybody once your four companies knew what you knew, how much faster would it have been than it was in the situation where you actually had prohibitions on the information sharing, intra-USG?

SMITH: Well, I think in this instance when we spoke to officials in one agency, typically within a day I think they spoke to officials in another. So, they understood and they were fast moving. I do think that one of the challenges in this space is the nature of all threat intelligence whether it's cyber based or physically based, is that it's always about connecting dots. So, the more dots you have, the more likely you are to see a pattern and reach a conclusion. And so, I think one of the challenges here is that the dots are so spread out. They're in a variety of different private companies, and they always will be. And then they're spread out across different parts of the public sector as well. So this notion of aggregating them is key.

The one thing that we haven't talked about though that I would add to this is there should be some level of information sharing in an appropriate way back to those of us in the private sector that really are first responders. I look at the Microsoft Threat Intelligence Center, and we are able to aggregate this data across our services. And you heard from CrowdStrike or FireEye, and they do similar things. But we too are operating with imperfect information when we don't have access to this knowledge. So, that's another key question I think that really merits consideration.

SASSE: I am over time but thank you to all four of you and I will follow up with somebody for more as well.

Thanks, Chairman.

WARNER: Well I want to thank all the witnesses, but I also want to make sure that people have hung in, if Senator Blunt, Senator Burr, and Senator Rubio, but I've got one more question, but I want to see if Senator Blunt, do you have anything else? Dianne, do you have? Richard? Marco?

RUBIO: I mean I think one of the things about this is corporations and government, they trust a number of software vendors now to run programs remotely in the cloud. They even allow them access to our networks to provide updates to help perform better for safety and so forth. So, this is really not just a national security thing, it really goes at the heart of how we conduct business across multiple sectors. By the way, i would venture to guess that most companies, mid-size companies and above have no idea how many different pieces of software. They don't know what their own inventory is, what they're running. So now is probably a good time to have someone in charge of knowing that in case something like this comes up.

I have three quick questions. On SolarWinds, I'm not sure I've heard yet, do we know what the initial entry point into the network was?

RAMAKRISHNA: Senator, our investigation on how, which is the initial entry point is still active at this point. We have had a number of hypotheses over the last couple of months working with our investigation partners. We've been able to narrow them down now to about three, which I hope will help us conclude to one. But just the nature of the investigation, as we are still sifting through terabytes of data, to figure out if we can pinpoint that particular one.

RUBIO: So TeamCity produced by JetBrains, any indication they could be one potentially?

RAMAKRISHNA: Senator, TeamCity is a tool used in the build processes by us and many other companies out there. We, to date, have no evidence that it was the back door used to get into SolarWinds. Although we haven't eliminated that possibility, we haven't proven it.

RUBIO: And on Microsoft, so far back as 2017 that the forged identity credentialing, you were aware of that vulnerability as far back as -- when were you aware of that and what was done -- what was done from the point you knew moving forward on the -- to address that?

SMITH: Well, the forged identity refers to an industry standard, SAML, the security -- it's a markup language. It's an industry standard that is supported by a wide variety of products including our own. Actually as we investigated this incident, we found that it was relevant in only 15 percent of the cases. And in those 15 percent in every instance, this tool was used to, in effect, add access capability only after the actor was in the network, had obtained access with what we call elevated privileges and was able to move around and then use this.

But to answer your question, this particular standard, the SAML standard, was created in 2007, so, long before 2017, we and many companies in the industry have been working to move people toward a more modern authentication standard, and there has been one that has been around since 2012, more broadly, independent of what security standard you use for this kind of authentication, the thing that we have been advising our customers and the practice that we have been following ourselves is really to do the following.

One, move your authentication service into the cloud. Number two, secure all of your devices. We have a service called InTune that does that. Number three, make sure you're using multifactor authentication. Number four, have what's called least privileged access, meaning don't give individuals access to the entire network or to be able to do things that they don't need to do. And number five, use a contemporary or modern antivirus or anti-Malware service like Windows Defender. And the reality is any organization that did all five of those things, if it was breached it in all likelihood suffered almost no...

RUBIO: Because it would have been contained or whatever in the department they entered.

SMITH: Absolutely. Yes. And these are five practices that the world knows about and this goes back, i think, to this point that we do need more Cybersecurity professionals to work with more organizations, and obviously it's incumbent on us, every day we're working to make it easier for our customers to deploy all of this.

RUBIO: And I think that just touches on the notion that even if you can't prevent the attack or the intrusion, you can mitigate its impact if you can do some of these things you've discussed.

And Mr. Mandia, this is my last question. We've talked about notification, not disclosure, but notification. And it seems to me that -- and you may have some thoughts on this -- but what is the threshold for that. Is it a major breach? Is it breach? Is it breaches that have indications of nation-state involvement? I mean, because I think every day someone is getting pinged by somebody, so...

MANDIA: I agree and you don't want to spread fear, uncertainty and doubt by folks who can't do a proper investigation or lack of expertise, or quite frankly they don't know what really happened, but they disclosed so fast that they do create unnecessary fear. That is the hardest part because every disclosure is going to have some discretion built into it. And that's why when I'm talking about information, I'm trying to -- there's public disclosure and legal disclosure. I'm trying to separate that.

And Brad Smith did in his testimony very well, to threat intelligence sharing and I'm more talking about threat intel, get it out there fast, get it out there confidentially so you have the time to figure out the threshold for disclosure. But that's a lot of work because I think it depends on the industry you're in whether you should disclose. I think if there's contract law that will apply you should disclose your customers, at least, that are impacted. But I still feel disclosure is always going to be based on impact of a breach which requires investigation.

**WARNER: Well, let me thank all of the panel and George, who's online. They actually had -- while Senator Risch did one last question we had full participation from the committee, and that is sometimes a rare occurrence. I take away four issues that I'd like for the record since it's been a long afternoon. The fact that Mr. Smith said this was potentially one of the most serious breaches he's seen, we know that it got into as what Mr. Ramakrishna's 18,000 customers. And while they chose to only exploit 100 plus, the fact that this could have been used not for exploitation and ex-filtration of information but could have been termed -- they were inside as I think Mr. Mandia so eloquently boot, it could have been exponentially worse. And I think we need to recognize the seriousness of that.**

**Number two, and I think Senator Rubio was raising this as well, that while it was a top tier nation state with their A team and it may be hard for any individual company or public enterprise to totally block that out, we can't default to the security fatalism. We've got to at least raise the cost for our adversaries and whether the items that Mr. Smith just enumerated in terms of better protections, even if they get in, we can find them and raise the costs if we think through this.**

**Mr. Smith commented on this, but I would like the rest of you for the record to comment on this, this idea around norms and international norms. I use the analogy that in warfare you don't bomb the ambulance. Well, should we try to get to a point that we don't bomb the patch or that you don't hit the hospital literally or the electoral systems? How do we move towards that system of norms?**

**And finally I think there is a real growing sense, and I hear this from industry as well, that we need some level of at least information sharing around on a mandatory basis.**

**Again, I want to compliment Kevin's company and Kevin personally for coming forward, because but for that effort we might still be -- this might still be ongoing. And how we think about that, what that reporting to or whom we report to mechanism I think is going to require some new creation. And while I am very open to some level of liability protection, I'm not interested in a liability protection that excuses the kind of sloppy behavior, for example, that took place in Equifax, where they didn't do the basic cyber hygiene, that if you report back, you should not be free of your responsibility if you have been a sloppy player. So I think there is -- there are models. there's FinCEN in the financial sector, there's the National Transportation Safety Board which may be an even better example I think that Mr. Mandia pointed out within the credit card arena. There is this information sharing.**

**Some, I know, have been thinking about the idea that the cloud service providers, the large enterprises, the first responders a la CrowdStrike and FireEye maybe being co-located at some location with parts of the government because this notion of getting the information out real time, that's not going to happen, with all due respect to the great talents that are at the FBI that's not going to happen, when it goes to the FBI and they're just not in the business of information sharing. And frankly, it's probably not going to happen, even though CISA's skills continue to be upgraded, we're going to have to think about a different model. And I challenge all of you to come forward with that.**

**I think there's a great deal of appetite, bipartisan appetite. I think we realize how serious we were and we potentially dodged a much more serious bullet and really appreciate all of your participation. And as has been mentioned constantly mentioned those companies that chose not to participate so far, we're going to give them another chance and hopefully they will recognize they have that kind of public service obligation that is reflected by the testimony today.**

**With that, the hearing is adjourned. Thank you.**

**END**

**Feb 24, 2021 12:45 ET .EOF**